情報処理学会論文誌 Vol.58 No.9 1388–1398 (Sep. 2017)

招待論文

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

笠間 貴弘[1,a)] 井上 大介[1,b)]

受付日 2017年2月9日, 採録日 2017年6月19日

概要：ここ数年 Web カメラや Wi-Fi ルータ，デジタルビデオレコーダといった IoT 機器がマルウェアに感染し，大規模な攻撃活動に悪用される事例が多発している．特に，昨年度発生した IoT 機器に感染するマルウェア Mirai のようにネットワーク経由で感染を拡げるタイプのマルウェアが猛威を振るっている．我々はインターネット上における広範囲な攻撃活動を把握するために約 30 万 IPv4 アドレスにおよぶ大規模なダークネットに届くトラフィックを観測・分析しているが，その観測においても多数の IoT 機器からとみられる攻撃活動をとらえている．一方で，効果的な対策導出のためには実際にマルウェア感染している機器を判別し被害状況を正確に把握することが重要だが，ダークネット観測のような受動的な観測手法から得られる情報だけでは攻撃元機器の判別までは困難である．そこで本稿では，ダークネットで観測された攻撃元機器に対するスキャンによって応答を収集し，それらを基に攻撃元機器の分類を行うことでマルウェア感染 IoT 機器の現状を明らかにする．

キーワード：IoT 機器，ダークネット観測，スキャン，クラスタリング

Clustering of Compromised IoT Devices based on Large-scale Darknet Monitoring and Active Scanning

Takahiro Kasama[1,a)] Daisuke Inoue[1,b)]

Received: February 9, 2017, Accepted: June 19, 2017

Abstract: In recent years, many cyber-attacks by abusing compromised IoT devices such as Web cameras and Wi-Fi routers have occurred. Although there are some analysis reports related to such cyber-attacks by security vendors, it is still unclear about global compromised IoT landscape. We have been observing many attacks from IoT devices in our darknet monitoring. However, only the information obtained from passive monitoring is not sufficient to distinguish actual infected devices. In this paper, we propose a clustering method of attacking devices combined large-scale darknet monitoring and active scanning for shedding light on current situation of compromised IoT devices.

Keywords: IoT device, darknet monitoring, active scanning, clustering

1. はじめに

2016 年 10 月 21 日に発生した DNS サービスを提供する Dyn 社に対する大規模な分散型サービス妨害攻撃（DDoS 攻撃）では，攻撃の影響で Twitter や PayPal といった著名なインターネットサービスへのアクセスが一時的に困難となる障害が発生した．セキュリティベンダや研究者によるレポートでは，この攻撃では Mirai と呼ばれるマルウェアに感染した世界中の Web カメラや Wi-Fi ルータといった IoT 機器が攻撃に悪用されたと報告されている [1], [2], [3]．従来，マルウェアの感染対象となるのは主に Windows OS が搭載された PC であり，特に能動的に次の攻撃先を探して感染を広めるワームタイプのマルウェアは世界中で数百万台規模の感染 PC を生み出すなど甚大な被害を発生させ

[1] 国立研究開発法人情報通信研究機構
National Institute of Information and Communications Technology, Koganei, Tokyo 184–8795, Japan
[a)] kasama@nict.go.jp
[b)] dai@nict.go.jp

ていた．しかし，Windows OS のセキュリティ向上とアンチウイルスソフトの普及やセキュリティに対するユーザ意識の高まりによって，Windows OS 自体に対する攻撃のハードルは上がっている．そのため，ここ数年のマルウェア感染の主要なターゲットとして新たに狙われるようになったのが，Web カメラや Wi-Fi ルータなどの IoT 機器である．これらの機器は組込み向け Linux OS の利用によるプラットフォームの共通化や機器の高性能化によって PC やサーバと実質的に大きな差異はない一方で，セキュリティ対策は十分に醸成されておらず，結果として攻撃者にとって格好の攻撃対象となっている．

インターネットにつながる大量の IoT 機器が容易にマルウェア感染してしまうことを示した最初の大規模な実例は 2012 年に登場した Carna [4] ボットネットである．Carna の感染方法は，Telnet サービス（23/TCP）に対するスキャンを行い，応答があったホストに対して典型的な ID とパスワードの組（ID とパスワードがともに admin など）を使って辞書攻撃を行い，ログインに成功すればマルウェア本体をダウンロードし実行するという単純な方法であった．しかしながら Carna 作成者が公開したレポートによればインターネット上の約 42 万台以上のデバイス（主にルータ）に対して Carna を感染させることができたと報告されている．本来，インターネットから機器に対する Telnet アクセスが可能であること自体がセキュリティの観点からは望ましくないが，それに加えてパスワードをデフォルト設定から変更していない機器が多数存在していることが明らかになった事例である．上記の DDoS 攻撃に用いられた Mirai も同様に Telnet 経由での感染によって広まっており，いまだに脆弱な機器が多数存在していることを示している．このような IoT 機器に感染を拡げるマルウェアや実際に感染させた IoT 機器を悪用した個々の攻撃事例については複数のレポート [5], [6], [7], [8] が報告されているほか，Mirai については作成者とみられる人物によってソースコードがインターネット上で公開されたことで，当該ソースコードを解析し感染活動の仕組みなどを調査した結果が公開されている [9], [10]．一方で，Telnet 以外のプロトコルによる感染拡大や，Mirai のソースコードを流用した新たなマルウェアの登場など，IoT 機器を取り巻く脅威と実際の感染機器の状況は変化し続けている．

我々は，主にインターネット上で能動的に感染を拡大するマルウェアの活動を把握するために大規模なダークネット観測を実施している [11] が，その観測においても多数のマルウェア感染 IoT 機器からとみられる攻撃活動をとらえている [12], [13], [14]．IoT 機器のマルウェア感染対策としては，すでに感染してしまった機器の特定や駆除，さらなる感染を防止するための製造メーカへの情報共有やパッチ作成などが重要となるが，多種多様な機器が存在し関係するメーカも多いため，より被害状況の大きな機器に対して優先的に対処していくことが効果的な対策につながると考えられる．しかしながら，ダークネット観測のような受動的な観測手法から得られる情報だけでは感染機器の判別までは困難である．そこで本稿では，ダークネットで観測された攻撃元機器に対して能動的なスキャンを行うことで得られた応答結果を分類する手法を提案し，実際の観測データに適用することでマルウェア感染 IoT 機器の現状を明らかにする．

本稿の構成は以下のとおりである．まず 2 章でダークネット観測でとらえた 2017 年以降の IoT 機器を狙った攻撃活動について示す．次に 3 章で能動的スキャンで得られた応答を基にした攻撃元機器の分類手法を説明し，4 章で実際の観測データに適用した結果を示す．5 章で関連研究について整理し，6 章でまとめとする．

2. ダークネット観測

ダークネットとはインターネット上の未使用かつ到達可能な IP アドレス空間を指す．通常，正規の通信が未使用の IP アドレス宛てに送信されることはないため，ダークネットで観測される通信はワームタイプのマルウェアが次の攻撃対象を探索するためのスキャンや送信元を詐称した DDoS 攻撃の跳ね返りなど何らかの不正な活動に起因するものである．そのため，大規模なダークネットに届く通信を観測・分析することで，インターネット上で発生している大規模なマルウェア感染や攻撃活動を把握する取組みが 2000 年台前半から行われている [11], [15], [16]．本章では，実際に IoT 機器を狙った大規模な攻撃活動が発生しており，それらがダークネットで観測されていることを確認するために，我々の NICTER プロジェクトで実施している約 30 万 IPv4 アドレスのダークネット観測の結果を示す．以降，“攻撃元ホスト数” とはユニークな送信元 IP アドレス数のことを指す．

2.1 IoT 機器に関連した攻撃活動の観測結果

現状の IoT 機器への主要な感染経路は Telnet であり，2016 年 9 月末にインターネットで公開された Mirai のソースコードにも，Telnet がデフォルトで利用するポート番号である 23/TCP に加えて，2323/TCP に対してもスキャンを行い感染を拡げる機能が備わっていた．そこでまず**図 1** に 2017 年 1 月 1 日から 5 月 10 日までの期間における，23/TCP および 2323/TCP に対する攻撃元ホスト数の推移を示す．図 1 を見ると，3 月以降に緩やかな減少傾向を示しているものの，23/TCP に関しては 5 月の段階でも 1 日に 40 万ホスト以上からのスキャンを観測しており，いまだに大量の感染機器が存在していることが分かる．なお，Mirai のソースコードではスキャンパケットの TCP ヘッダのシーケンス番号に宛先 IP アドレスと同じ値が利用されるという特徴があったが，2017 年以降に観測され

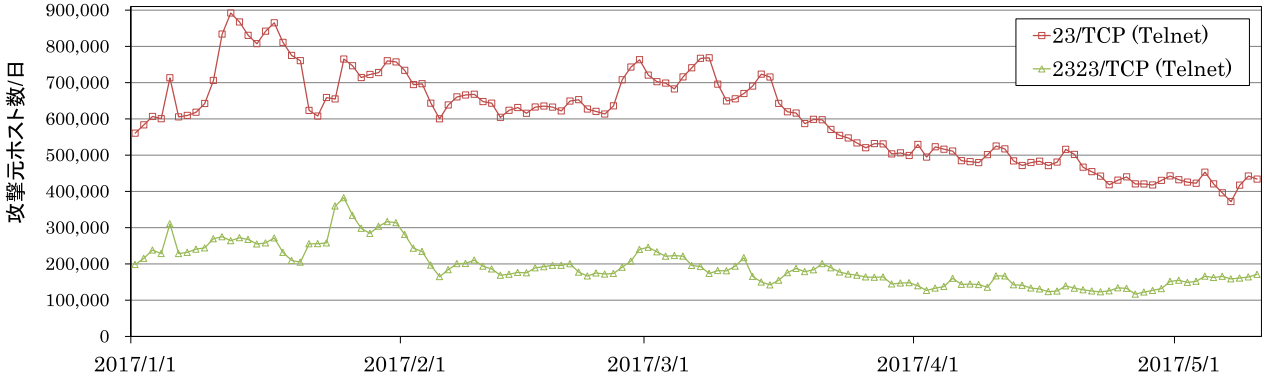

図 1 ダークネットで観測された日毎の攻撃元ホスト数（23/TCP, 2323/TCP）

Fig. 1 Number of scanning hosts captured via darknet (23/TCP, 2323/TCP).

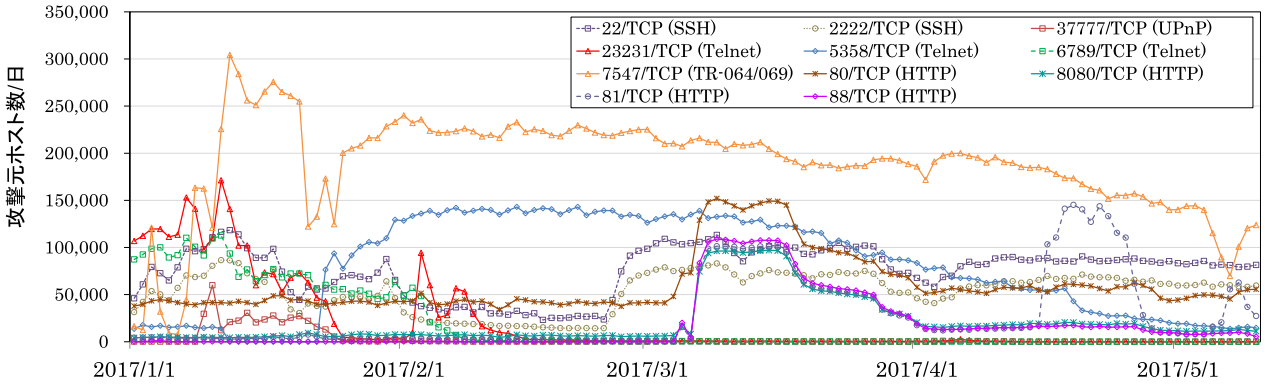

図 2 ダークネットで観測された日毎の攻撃元ホスト数（IoT 機器に関連した宛先ポート）

Fig. 2 Number of scanning hosts captured via darknet (IoT related ports).

た 23/TCP への攻撃元ホストについては，この特徴的なパケットを送信しているホストは全体の約半数程度しか観測されておらず，Mirai 以外のマルウェアに感染している IoT 機器も多数存在していることが推測される．

次に，**図 2** に IoT 機器に関連した攻撃活動のうち，上記ポート番号以外で 2017 年以降に活発な攻撃活動を観測した 11 個のポート番号に対する攻撃元ホスト数の推移を示す．IoT 機器に関連した攻撃活動か否かの判断は，観測されたパケットの特徴や攻撃元ホストの調査，他組織からのレポートなどから判断している．

22/TCP と 2222/TCP は SSH を狙った攻撃活動である．これらのポート番号に対するスキャンは 2016 年 6 月に一度急増し，それ以降は 1 日に 2 万ホスト前後が観測されていたが，2016 年 12 月 25 日に再度攻撃元ホスト数の急増を観測した．同時期に SSH に対するブルートフォース攻撃によって IoT 機器に感染を広めるマルウェア [17] が報告されており，このマルウェアの感染拡大によって観測数が増加したと考えられる．攻撃元ホスト数は 2017 年 1 月末にいったん減少したものの 2017 年 2 月末に再度急増し，現在も 1 日に 8 万ホスト以上が観測されている．

37777/TCP は海外製のデジタルビデオレコーダなどで利用されており 2016 年 12 月 10 日に攻撃元ホスト数の急増を観測していた．警察庁のレポートでは，37777/TCP へのアクセスは UPnP によって 23231/TCP 経由での Telnet アクセスを可能にするための設定変更を試みるものだと報告されている [18]．実際に 23231/TCP に対する攻撃元ホスト数も同時期に急増を観測していることからレポートと同一の事象だと考えられる．現在ではこれらのポート番号に対する攻撃活動は終息している．

5358/TCP と 6789/TCP に対する攻撃活動はどちらも当該ポートで Telnet を動作させている特定の IoT 機器を狙った攻撃活動である．6789/TCP に関しては Dahua 社製のデジタルビデオレコーダを狙った攻撃活動であるという報告があり [19]，2016 年 12 月 18 日に攻撃元ホスト数の急増が観測されたが現在は終息している．5358/TCP も複数の IoT 機器が利用しているという報告があり [20]，我々の観測では 2016 年 12 月 24 日から 2017 年 1 月 11 日かけて攻撃活動が観測された後，2017 年 1 月 23 日に再度急増を観測した．その後はゆるやかに減少傾向を示し，5 月 10 日の時点では 1 日に 1.5 万ホスト程度が観測されている．

7547/TCP は TR-064/069 で利用されているポート番号であり，2016 年 11 月 27 日にドイツの ISP である Deutsche Telekom 社の顧客に設置している DSL モデム/ルータに対して当該サービスの脆弱性を悪用した攻撃が発生し，大規模な障害が発生した [21]．我々の観測でも，同時期に 250 万ホスト以上から非常に大規模な攻撃活動を観測してお

表 1 各ポート番号に対する攻撃元ホストの国分布
Table 1 Country distribution of attacking hosts on each destination port.

23/TCP (Telnet)		2323/TCP (Telnet)		22/TCP (SSH)		2222/TCP (SSH)		5358/TCP (Telnet)	
国	ホスト数 (割合)	国	ホスト数 (割合)	国	ホスト数 (割合)	国	ホスト数 (割合)	国	ホスト数 (割合)
イラン	57,366(13.2%)	ロシア	27,923(16.3%)	ロシア	15,586(19.1%)	アルゼンチン	12,190(20.4%)	ブラジル	3,088(21.0%)
ロシア	55,808(12.9%)	インド	22,938(13.4%)	エクアドル	13,685(16.8%)	ロシア	11,820(19.8%)	インド	2,115(14.4%)
インド	46,390(10.7%)	中国	22,305(13.0%)	アルゼンチン	13,492(16.6%)	エクアドル	10,154(17.0%)	ベトナム	1,227(8.4%)
ブラジル	45,785(10.6%)	ブラジル	20,049(11.7%)	ブラジル	9,672(11.9%)	インド	5,133(8.6%)	韓国	1,115(7.6%)
中国	40,283(9.3%)	アルゼンチン	13,486(7.9%)	インド	6,683(8.2%)	中国	4,594(7.7%)	中国	702(4.8%)

7547/TCP (TR-064/069)		80/TCP (HTTP)		81/TCP (HTTP)		88/TCP (HTTP)		8080/TCP (HTTP)	
国	ホスト数 (割合)	国	ホスト数 (割合)	国	ホスト数 (割合)	国	ホスト数 (割合)	国	ホスト数 (割合)
イラン	46,375(37.5%)	アメリカ	23,011(41.3%)	中国	16,250(59.6%)	タイ	1,211(22.3%)	アメリカ	3,918(35.5%)
オーストラリア	10,515(8.5%)	ブラジル	7,820(14.1%)	タイ	1,964(7.2%)	インドネシア	1,054(19.4%)	ブラジル	1,204(10.9%)
. イタリア	8,890(7.2%)	中国	6,438(11.6%)	インドネシア	878(3.2%)	メキシコ	501(9.2%)	タイ	761(6.9%)
ロシア	8,225(6.6%)	イラク	2,307(4.1%)	アメリカ	845(3.1%)	アメリカ	364(6.7%)	中国	756(6.8%)
インド	6,505(5.3%)	ドイツ	1,065(1.9%)	メキシコ	836(3.1%	シンガポール	238(4.4%)	インドネシア	674(6.1%)

り，その後観測数は減少したものの 5 月 10 日時点でも 10 万ホスト以上が観測されている．

80/TCP，81/TCP，88/TCP，8080/TCP は HTTP を狙った攻撃活動である．4 月 24 日に中国のセキュリティ企業が 81/TCP 経由で IoT 機器に感染を拡げるマルウェア [22] に関する分析結果を公開しており，当該マルウェアは 3 月 8 日に公開された多数の Web カメラに存在する複数の脆弱性 [23] のうちの認証回避の脆弱性（CVE2017–8225）を悪用して感染すると報告されている．図 2 を見ると，我々の観測でも 3 月 8 日の脆弱性報告と同時期に 81/TCP に対する攻撃活動の急増を観測していることが分かる．さらに 81/TCP に加えて他の 3 つのポート番号に対する攻撃活動も急増していた．これは機器によって利用しているポート番号が異なる場合を想定し，候補となる複数のポート番号を攻撃対象としていると推測される．

以上のダークネット観測の結果から，Telnet に限らず，SSH や HTTP，UPnP など様々なプロトコルを通じた IoT 機器への攻撃活動が発生しており，マルウェア発生や脆弱性の報告に合わせてダークネット観測においても数万から数十万ホスト規模の攻撃活動が観測されていることが明らかになった．

2.2 攻撃元ホストの分布状況

5 月 10 日に観測された各宛先ポート番号に対する攻撃元ホストについて，攻撃元ホストの国分布を**表 1** に示す．ただし，5 月 10 日時点ですでに攻撃活動がほとんど観測されていない 6789/TCP，23231/TCP，3777/TCP は除外した．送信元 IP アドレスからそのホストが存在する国や ISP（Internet Service Provider）の情報を得るために GeoIP データベース [24] を利用している．

表 1 を見ると，各ポート番号によって攻撃元ホストの国分布が大きく異なっていることが分かる．たとえば，23/TCP と 7547/TCP に関しては最も攻撃元ホストが多い国はイランとなっており，23/TCP では全体の 13.2%，7547/TCP では全体の 37.5%を占めている．従来の Windows OS を狙った攻撃活動では中国やロシアといった国が上位を占めており，イランからの攻撃活動はあまり観測されてはいなかったため，これは IoT 機器に関連した攻撃活動に特徴的な傾向である．その他に，22/TCP と 2222/TCP に関してはロシアに加えて，アルゼンチンやエクアドルといった南米の国の割合が高く，80/TCP や 8080/TCP ではアメリカとブラジルで半数近くを占めている．このようにポート番号ごとに攻撃元ホストの国分布が大きく異なっている理由としては，当該ポート番号経由で感染可能な機器の流通地域が影響していると考えられる．たとえば 81/TCP に対する攻撃元ホストの 6 割近くが中国であるが，これは脆弱性を有する機器の多くが中国のメーカが製造した Web カメラであると報告されている [23] ことから，当該製品が中国内で流通しマルウェア感染している可能性が高いと推測できる．なお，81/TCP に関しては日本の攻撃元ホスト数が 325 IP アドレスと全体の 10 番目に多く観測されており，国内でも該当する製品が一定数流通しており感染している可能性が高い．

国よりも細かな分布を把握するために，表 1 で上位を占めていた各国について 10 個の宛先ポート番号に対する攻撃元ホスト全体の属する ISP の分布を**表 2** に示す．表 2 を見ると，各国ともに特定の ISP に攻撃元ホストが集中していることが分かる．特にロシアやアルゼンチンなどでは 8 割以上の攻撃元ホストが 1 つの ISP に属している．なお，中国に関しては GeoIP の検索の際に地域名も含まれた ISP 名が出力されるためそれぞれの割合は小さくなっているが実際には China Telecom と China Unicom が 9 割以上を占めている．このように特定の ISP に攻撃元ホストが集中している理由としては，各国における各 ISP のシェア（ユーザ数）の影響もあるが，Deutsche Telekom 社の事例のように ISP が顧客に配布している機器が感染している可能性も十分に考えられる．ISP ではなく攻撃元ホストをクラス B（/16）ネットワークごとに集計した際の累積分布関数（CDF）を**図 3** に示す．図 3 を見ると全体の攻撃元ホストのうち，94 個のクラス B ネットワークで全体の 2 割，

表 2 各国の攻撃元ホストの ISP 分布
Table 2 ISP distribution of attacking hosts in each country.

イラン		ロシア		アルゼンチン	
Iran Telecommunication Company PJS	23,448(36.6%)	Rostelecom	51,432 (85.4%)	Telefonica de Argentina	16,698(82.1%)
Information Technology Company (ITC)	22,927(35.8%)	JSC ER-Telecom Holding	881 (1.5%)	Telecom Argentina S.A.	908(4.5%)
Asiatech Data Transfer Inc PLC	4,873(7.6%)	PJSC Bashinformsvyaz	711 (1.2%)	Cablevision S.A.	590(2.9%)

ブラジル		アメリカ		中国		タイ	
Vivo	16,893(26.5%)	Comcast Cable	7,076(21.8%)	China Unicom Liaoning	6,558(10.3%)	TOT	4,023(37.8%)
Oi Internet	16,729(26.2%)	Time Warner Cable	3,906(12.0%)	China Telecom jiangsu	5,251(8.2%)	3BB Broadband	3,183(29.9%)
Oi Velox	6,812(10.7%)	AT&T U-verse	3,745(11.5%)	China Telecom fujian	4,893(7.7%)	True Internet	1,491(14.0%)

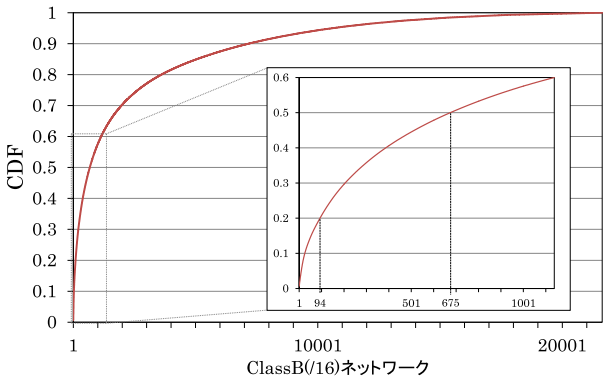

図 3 クラス B（/16）単位の攻撃元ホスト数分布
Fig. 3 CDF of the attacking hosts in /16 networks.

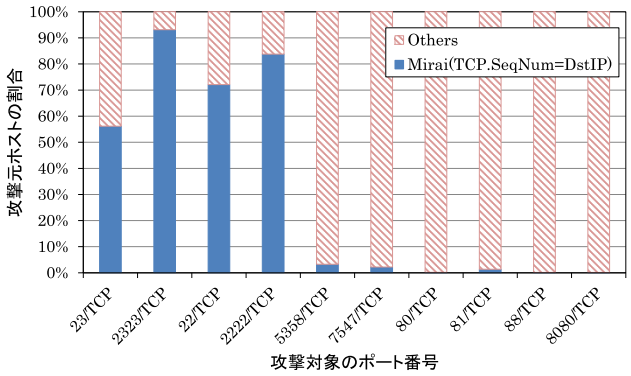

図 4 Mirai の特徴を有する攻撃元ホストの割合
Fig. 4 Stacked chart on the scanning hosts (Mirai scanners vs. others).

675 個で全体の半数を占めており，特定のネットワークに攻撃元ホストが集中していることが分かる．中には 1 つのクラス C（/24）ネットワークのうちの 253 IP アドレスからの攻撃を観測しているケースも存在した．

2.3 Mirai の影響

2016 年 9 月末に Mirai のソースコードがハッカーフォーラムに公開されたことで，Mirai のソースコードを流用して作成されたとみられるマルウェアが多数登場している．そこで，実際にどの程度 Mirai もしくは Mirai のソースコードを流用したマルウェアの攻撃活動が観測されているか把握するために，**図 4** に 5 月 10 日に観測された上記の 10 ポート番号に対する攻撃元ホストについて，Mirai のスキャンの特徴である TCP ヘッダのシーケンス番号と宛先 IP アドレスの値が一致しているパケットを送信している攻撃元ホストの割合を示す．図 4 を見ると，公開された Mirai のスキャン対象である 23/TCP や 2323/TCP の攻撃元ホストについてはやはり Mirai の特徴を有する攻撃元ホストが半数以上を占めており，2323/TCP に関しては 9 割に達している．また，SSH に関連した 22/TCP や 2222/TCP についても，7 割から 8 割の攻撃元ホストが Mirai の特徴的なスキャンを行っており，Mirai に関連したマルウェアが感染活動を行っていると考えられる．一方で，5358/TCP や 7547/TCP，80/TCP などに対する攻撃ホストでは，Mirai の特徴を有する攻撃元ホストはほぼ観測されておらず，当該ポート番号に関しては Mirai とは異なるマルウェアが感染を拡げていることが分かった．

3. 攻撃元機器の分類手法

ここまで示したとおり，ダークネット観測を用いることで攻撃元ホストの規模や分布，マルウェアに特徴的なスキャンパターンなどの判定が可能になる．しかし一方で，実際にどのような機器がマルウェア感染の被害を受けているのかをダークネット観測で得られる情報のみから判断するのは困難である．そこで本章では，感染機器の分布状況を明らかにするために，観測された攻撃元機器に対して能動的なスキャンを行い，得られた応答を基に機器の分類する手法を提案する．

提案手法では，まず観測された攻撃元機器に対して複数のポート番号（サービス）へのアクセスを行い，機器からの応答を収集する．なお，インターネット全域に対してスキャンを行うことでインターネットからアクセス可能な様々な機器を探索する取組み [25], [26], [27] も存在するが，その結果見つかった機器が必ずしも脆弱でありすでにマルウェア感染しているわけではないため，能動的なスキャンだけでマルウェア感染状況を把握することは困難である．そのため我々は，ダークネット観測によって攻撃活動が観測された機器のみに限定して応答を収集することで，実際にマルウェアに感染し攻撃活動に悪用されている機器の状況を把握する取組みを行っている [13], [14].

次に，各機器から収集した応答について類似度を算出し機器の分類を行う．ここでは，同一の機器（たとえば同じ型番のルータやWebカメラなど）であれば設定やアクセスのタイミングなどで多少変更される部分が存在しても全体としては類似した応答が返ってくると仮定し，応答の類似度が高いものを同一の機器とみなす．前述のインターネット全域に対するスキャンを行っているプロジェクトなどでは，応答の中に含まれる機器特有の情報（たとえば，Telnetのログインバナーに含まれる型番情報など）をシグネチャとして利用することで同一の機器を探索する取組みが行われているが，実際に流通している機器は多岐にわたるためすべての機器に対してシグネチャを生成することは容易ではない．そのため我々の取組みとしては，シグネチャによらない類似度に基づいて分類を行うことで，まずは全体の感染状況を把握することを目指す．それによって感染規模の大きな機器から優先的に対策を行うような取組みが可能になる．

類似度の算出については，1つの機器上で複数のサービスが異なるポート番号で稼働している場合があり，またサービスによって応答フォーマットやデータサイズが異なるため，提案手法では汎用的な類似度算出手法として正規化圧縮距離（NCD：Normalized Compression Distance）[28]を利用する．NCDは，背景知識を必要とせずデータ間の類似度を測る汎用な尺度である正規化情報距離（NID：Normalized Information Distance）[29]におけるKolmogorov Complexityを現実の圧縮アルゴリズムで代替したものである．NCDはある圧縮アルゴリズムCによって文字列xを圧縮したときの圧縮長を$C(x)$とすると，以下の式で表される．

$$NCD(x,y) = \frac{C(xy) - \min\{C(x), C(y)\}}{\max\{C(x), C(y)\}}$$

ここで，xとyの2つの機器に対してある宛先ポート番号（サービス）pへのスキャンによって得られた応答x_p，y_pの類似度S_pをNCDを用いて以下の式で与え，最終的な2つの機器の類似度$S(x,y)$はスキャン対象としたすべてのポート番号のうち，両機器からともに応答が得られたポート番号からの応答の類似度の平均値とする．なお，片方のみもしくは両方とも応答が得られなかったサービスは除外する．

$$S_p = 1 - NCD(x_p, y_p)$$

$$S(x,y) = \frac{1}{|P|}\sum_{p \in P} S_p$$

クラスタリングについては，事前に機器の種類数（クラスタ数）を判断することが困難なため，群平均法を用いた階層的クラスタリングによって機器の分類を行う．

4. 実験結果

本章では，提案手法を実際の観測データに適用した結果を示す．ダークネットで観測されるのは主に能動的に感染を拡げるワームタイプのマルウェアの活動であるため，IoT機器を狙った攻撃元ホストの多くはすでにマルウェアに感染したIoT機器である可能性が高いと考えられる．そこで，2章で示したIoT機器に関連した攻撃活動における攻撃元ホストに対して提案手法を適用することでIoT機器の感染状況を把握する．

4.1 能動的スキャンによる応答収集

まず，2017年5月10日のダークネット観測の結果から，10個の宛先ポート番号（23/TCP，2323/TCP，22/TCP，2222/TCP，5358/TCP，7547/TCP，80/TCP，81/TCP，88/TCP，8080/TCP）について攻撃元ホストを抽出した．各宛先ポートに対する攻撃元ホスト数はそれぞれ，433,786 IPアドレス（23/TCP），171,160 IPアドレス（2323/TCP），81,446 IPアドレス（22/TCP），59,609 IPアドレス（2222/TCP），14,677 IPアドレス（5358/TCP），123,724 IPアドレス（7547/TCP），55,651 IPアドレス（80/TCP），27,276 IPアドレス（81/TCP），5.437 IPアドレス（88/TCP），11,041 IP（8080/TCP）であった．

抽出した各ホスト（重複を除いたユニーク数で556,693 IPアドレス）に対して，上記10個のポート番号にFTP（21/TCP）を加えた計11個のポート番号に対して5月13日にスキャンを行い，応答を収集した．スキャンにはネットワークスキャンツールであるNmap [30]とその拡張機能であるbanner–plus [31]を利用した．スキャンではセッションを確立すると，HTTPで利用されるポート番号の場合はGETリクエストを送信し応答を収集する．それ以外のポート番号では何も送信せず5秒間応答を待機したあと，何も受信しなかった場合はGETリクエストを送信し再度応答を待つ．banner–plusはTelnetやSSH，FTPなどのプロトコルの応答を受信した際には適切に返答しバナー情報を収集することができる．

スキャンの結果，全体の26.7%（148,583 IPアドレス）のホストについては，スキャンによって1つ以上のポート番号へのアクセスが可能であった．また，そのうちの約3割（43,797 IPアドレス）のホストについては2つ以上のポートに対してアクセスが可能であったことから，インターネットに対して複数ポートを開放している機器が一定数存在しており，複数ポートからの応答を組み合わせることでより正確な機器特定につなげられると考えられる．

スキャンの結果を**図5**に示す．図5では横軸にスキャンしたポート番号を示し，縦軸に抽出した各攻撃元ホストのうちアクセス可能であったホストの割合を示している．たとえば，図5の横軸が23/TCPの位置にある各棒グラ

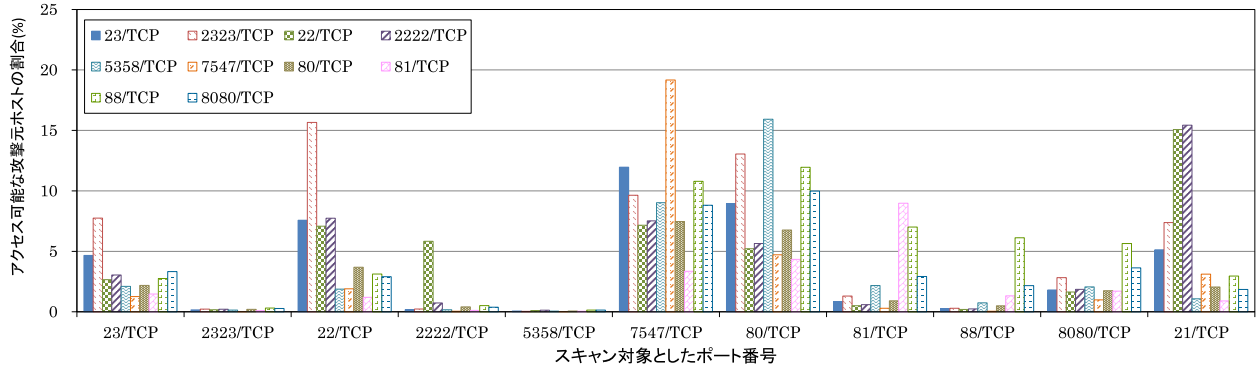

図 5 各ポート番号に対する能動的スキャンでアクセスできた攻撃元ホストの割合

Fig. 5 Percentage of attacking hosts accessible by active scanning.

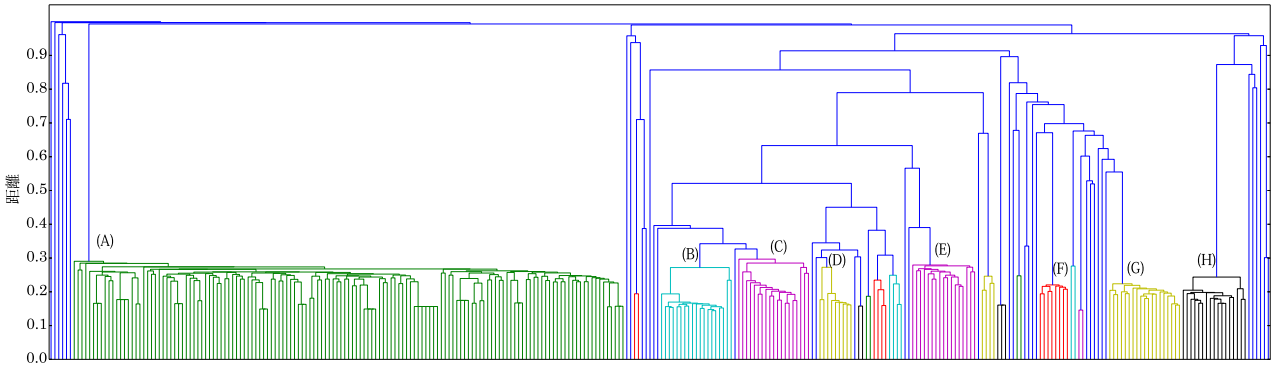

図 6 日本国内の攻撃元ホストの分類結果

Fig. 6 Clustering result of attacking hosts in Japan.

フは，ダークネットで観測された各宛先ポートに対する攻撃元ホストのうち，こちらから 23/TCP でアクセス可能であったホストの割合を示している．最も左の棒グラフを見ると，ダークネットで観測された 23/TCP に対する攻撃元ホストのうち，4.7%のホストは 23/TCP でアクセスが可能であることが分かる．順に右の棒グラフを見ていくと，2323/TCP に対する攻撃元ホストでは 7.7%，22/TCP に対する攻撃元ホストでは 2.7%，2222/TCP に対する攻撃元ホストでは 3.0%という結果を示している．図 5 を見ると，各ポートに対する能動的なスキャンではいずれもアクセス可能なホストは 2 割以下と少ない割合となっており，特に 2323/TCP や 5358/TCP などのポート番号でアクセス可能なホストはほとんど居ないことが分かる．2015 年に我々が同様の調査を行った際には 23/TCP への攻撃元ホストのうち約 16%が 23/TCP でアクセス可能であり [13]，そのときからさらに減少している状況が明らかになった．これは，Mirai をはじめとするここ数年のマルウェアの多くが，感染に成功した際に他のマルウェアの感染を防いだり管理者からのアクセスを遮断する目的で，感染時に利用したサービスを含めた複数のサービスを停止する機能を備えており，その影響によってアクセスができないホストが増加している可能性が高い．一方，他のポート番号と比べて 7547/TCP や 80/TCP などへのスキャンは比較的アクセス可能なホストの割合が多く，Telnet ほどマルウェアによるサービス停止が行われていない状況が分かる．

4.2 攻撃元機器の分類

最後に，収集できた応答を利用して攻撃元機器の分類を行う．本稿ではクラスタリング結果に対して手動での確認を行えるように，日本国内の攻撃元ホストのみに絞って分類を行い，分類結果の妥当性を検証する．日本国内の攻撃元ホストは 771 IP アドレス存在し，そのうち能動的スキャンによって 1 つ以上のサービスから応答が得られたものは 316 IP アドレスであった（そのうち，2 つ以上のサービスから応答が得られたものは 53 IP アドレス）．各ポート別でみると，23/TCP でアクセス可能なホストが 6 IP アドレス，22/TCP が 87 IP アドレス，7547/TCP が 1 IP アドレス，80/TCP が 95 IP アドレス，81/TCP が 143 IP アドレス，88/TCP が 3 IP アドレス，8080/TCP が 4 IP アドレス，21/TCP が 24 IP アドレス，そのほかのサービスでは応答が得られたホストは存在しなかった．これらのホストからの応答について類似度計算を行いクラスタリングを行った．なお，NCD の計算における圧縮アルゴリズムは bzip2 [32] を用い，クラスタリングの計算には Python ライブラリの SciPy [33] を利用した．分類結果のデンドログラムを図 6 に示す．デンドログラムの図を基に，今回はヒューリスティックにクラスタリングの閾値を 0.3 と決め，各クラスタを色分けしている．閾値を 0.3 とした場合，

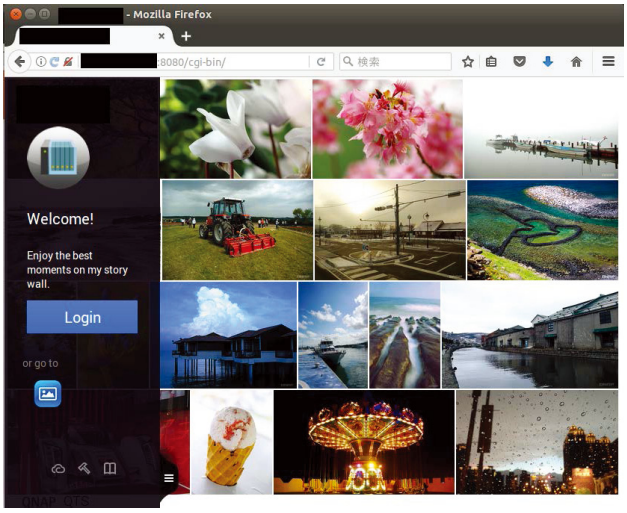

図 7 感染機器（NAS）の WebUI 画面
Fig. 7 Web interface of infected network attached storage.

316 IP アドレスが 56 のクラスタに集約され，そのうち 38 クラスタについては単一のホストのみのクラスタとなった．

ここで実際に，同様の機器が適切に同じクラスタに集約されているかを確認するため，図 6 の中でノード数の多い各クラスタ（図中の (A) から (F)）について手動で中身を精査した．

まず，最も多い 143 ホストが含まれていた (A) のクラスタには 81/TCP でアクセス可能な全攻撃元ホストが含まれていた．各ホストから収集された応答を確認したところすべて GET リクエストに対する 401 エラーであったが，応答の中身に “GoAhead” の文字列が含まれており，レポート [23] で報告された対象の機器の可能性が高い．ただし，実際にはレポートで報告された製品は OEM 製品として複数の機器が存在しているが，応答の中身を確認した限りではその機器の違いまでを判断できるような情報は含まれていなかった．

(B)，(D)，(E) のクラスタはそれぞれ 22/TCP でアクセス可能な攻撃元ホストが含まれており，スキャンによって SSH のバナーが収集されていた．クラスタごとにホストの応答を確認したところ，それぞれのクラスタでは OpenSSH のバナーに含まれるバージョン情報が異なっており，その差異が影響して異なるクラスタに分かれていた．しかしながら，これらの機器に関しては収集されたバナーには機器の違いまでを判別できるような情報は含まれておらず，各クラスタの機器が同一の機器であるかは判断ができなかった．

(C) のクラスタは 19 ホストが含まれており，それらは FTP や HTTP などの複数ポートでのアクセスが可能なホストが含まれていた．実際にこれらのホストに対して HTTP でのアクセスを行うと，特定の NAS（Network Attached Storage）製品の管理画面（**図 7**）が閲覧でき，このクラスタに含まれているホストはすべて当該製品であった．

(F) のクラスタは 8 ホストが含まれており，80/TCP でのアクセスが可能なホストが含まれていた．それらの応答を確認したところ，応答の中にある特定の無線 LAN ルータの型番を示す文字列が含まれており，これらのホストはすべて当該製品であった．

(G) のクラスタは 19 ホストが含まれており，(F) のクラスタのホストと同様に 80/TCP でのアクセスが可能なホストが含まれていた．それらのホストはすべてトップページの GET リクエストに対して “/web/index.html” へとリダイレクトする応答を返していた．そのリダイレクト先にアクセスするとある特定の Web カメラのログイン画面が確認できた．

(H) のクラスタは 17 ホストが含まれており，8080/TCP でアクセス可能なホストが含まれていた．当該ポートにアクセスするとディレクトリのフォルダ一覧が閲覧でき，その中にあるメーカのロゴ画像ファイルなどが含まれており，それらのホストが当該メーカの機器であることが確認できた．

4.3 実験まとめ

ダークネットで観測した攻撃元ホストへのスキャンでは，マルウェア自身が感染機器上のサービスを止める影響もあり，応答を得られる攻撃元ホストの割合が少ないことが明らかになった．しかし，サービスによっては比較的多くのホストから応答が得られるものもあるため，脆弱性のあるサービスに限定せずスキャンを行うことでより多くの応答を収集できる可能性があり，分類可能な機器が増加すると考えられる．

クラスタリングに関しては，各クラスタに含まれるホストについて手動で応答を確認した結果，ホストの大きなクラスタについては実際の応答に応じて，同一のポート番号からの応答であっても製品やバージョンに応じて適切に分類されており，提案手法が期待したとおりの結果を得られていることを確認できた．ただし，同一の製品が OEM として展開されている場合などでは，特に単一のサービスから収集できる応答の中にそれらの差異を判断できるだけの十分な情報が含まれていない場合もあったため，複数のサービスからの応答を基に類似度を算出するなどの必要がある．

一方で，単一のホストしか含まれていない 38 個のクラスタについてもそれぞれを調査した結果，本来であれば同一のクラスタとして集約されるべき同一の機器からの応答と推測されるものが異なるクラスタに分かれているケースが存在した．この原因を調査した結果，データによっては bzip2 を用いた正規化圧縮距離の算出において非常に類似したデータであっても距離が大きくなってしまう場合があることが分かった．bzip2 の代わりに Lempel-Ziv-Markov chain-Algorithm を利用した xz 圧縮，Deflate を利用した

gzip 圧縮などを利用してもほぼ同様の結果となっており，より収集データに適した圧縮アルゴリズムの検討が今後の課題である．

5. 関連研究

IoT 機器に関するセキュリティ上の脅威や課題については様々な議論が存在する [34], [35] が，ここでは IoT 機器に関する攻撃活動の観測と IoT マルウェアの収集・分析について関連研究を整理する．

5.1 ダークネット観測・分析

ダークネット観測はインターネット上における大規模な攻撃活動をとらえるのに適した観測手法である．特に，ネットワーク経由で感染を拡げるワームタイプのマルウェアが大量感染を引き起こした際には，ダークネットで観測される攻撃元ホスト数の急増が観測されるため，過去にも Witty ワーム [36] や Conficker ワーム [37]，Carna ボットネット [12] といったマルウェアの感染活動の分析に用いられている．ワームタイプのマルウェアの多くはインターネット上をランダムにスキャンしていくため，ダークネットの観測規模が大きいほど確率的に多くの攻撃活動をとらえることができる．Moore らはダークネットの観測規模が観測結果に与える影響について考察している [15]．また，Wustrow らは 4 つのクラス B ネットワークという非常に大規模なダークネットで観測されたデータの分析を行っている．

5.2 能動的スキャンによる観測

インターネットからアクセス可能な機器を探索する単純な手法はインターネット全域に対して能動的にスキャンを行うことである．ミシガン大学で開発された Zmap [38] はオープンソースのネットワークスキャナであり，従来のスキャナと比較して非常に高速に動作し，条件によっては 1 台のマシンから 45 分で IPv4 空間すべてに対してスキャンが可能だと報告されている．こうしたツールは有効な反面，攻撃側も容易に利用が可能であるため，Zmap が公開されて以降，我々のダークネット観測においても Zmap を利用したと思われるスキャン活動を多く観測している．また，スキャンした結果をインターネット上で公開しているサービスも複数存在しており，その中の 1 つである Shodan [26] は IoT 機器で利用されているサービスについてスキャンを行い結果を公開している．そのため，利用者は自らスキャンを行うことなく容易にインターネットにつながる様々な機器の検索が可能となっている．

5.3 IoT マルウェアの収集・分析

マルウェア感染後の脅威を把握するためには，実際に IoT 機器に感染するマルウェアを収集し分析することが必要である．マルウェアを収集するためのシステムとして，IoT 機器に対する主要な感染経路である Telnet や SSH に対応したオープンソースのハニーポットである Cowrie [39] が存在する．また PaPa らは IoT マルウェアの収集と分析を行う IoTPOT を提案している [40]．IoTPOT では実際の機器から収集したバナー情報を攻撃元に対して変更することで実際の機器らしく振舞い，送り込まれたコマンドを解釈してマルウェア検体を収集する．IoTPOT を用いて収集されたマルウェアを解析した結果，DoS 攻撃を行う挙動や感染機器上に正規の Web サイトを模した偽サイトが構築される挙動などが報告されている．

6. まとめ

近年，大量の IoT 機器がマルウェアに感染し大規模な攻撃活動に悪用されるなどの被害が発生している．これら IoT 機器のマルウェア感染対策においては，すでに感染してしまった機器の特定や駆除，さらなる感染を防止するための製造メーカへの情報共有やパッチ作成などが必要であるが，多種多様な機器が存在し関係するメーカも多いため，より感染台数規模の大きな機器に対して優先的に対処していくことが効果的な対策につながる．これに対し，ダークネット観測はインターネット上で広範囲にスキャンを行うマルウェアの感染活動を把握する有効な手法であるが，そこから得られる情報だけでは実際にマルウェア感染している機器まで判別することは難しい．そこで本稿では，ダークネットで観測された攻撃元ホストに対してスキャンを行い，得られた応答から正規化圧縮距離を用いて同一の機器を分類する手法を提案した．提案手法を実際に観測された日本国内の攻撃元ホストに対して適用した結果，同一の機器や製品が適切に分類されていることを確認した．提案手法により各機器の感染台数の規模を把握することが可能になるため，対策に向けた状況把握に有効である．

参考文献

[1] Hilton, S.: Dyn Analysis Summary Of Friday October 21 Attack, available from ⟨https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/⟩ (accessed 2017-05-31).
[2] FP_Analyst: Mirai Botnet Linked to Dyn DNS DDoS Attacks, available from ⟨https://www.flashpoint-intel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/⟩ (accessed 2017-05-31).
[3] KrebsonSecurity: DDoS on Dyn Impacts Twitter, Spotify, Reddit, available from ⟨https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/⟩ (accessed 2017-05-31).
[4] Anonymous: Internet Census 2012 Port scanning /0 using insecure embedded devices, available from ⟨http://census2012.sourceforge.net/paper.html⟩ (accessed 2017-05-31).
[5] Xiao, C., Zheng, C. and Jia, Y.: New IoT/Linux Malware Targets DVRs, Forms Botnet, available from

⟨http://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/⟩ (accessed 2017-05-31).
[6] Grange, W.: Hajime worm battles Mirai for control of the Internet of Things, available from ⟨https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things⟩ (accessed 2017-05-31).
[7] Ducklin, P.: Deutsche Telekom outage: Mirai botnet goes double-rogue, available from ⟨https://nakedsecurity.sophos.com/2016/11/29/deutsche-telkom-outage-mirai-botnet-goes-double-rogue/⟩ (accessed 2017-05-31).
[8] Trend Micro USA: BrickerBot Malware Emerges, Permanently Bricks IoT Devices, available from ⟨https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/brickerbot-malware-permanently-bricks-iot-devices⟩ (accessed 2017-05-31).
[9] 株式会社インターネットイニシアティブ：Internet Infrastructure Review (IIR) Vol.33, available from ⟨http://www.iij.ad.jp/company/development/report/iir/033/01_04.html⟩ (accessed 2017-05-31).
[10] Roses, S.: Mirai DDoS Botnet: Source Code & Binary Analysis, available from ⟨http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/⟩ (accessed 2017-05-31).
[11] Inoue, D., Eto, M., Yoshioka, K., Baba, S., Suzuki, K., Nakazato, J., Ohtaka, K. and Nakai, K.: nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis, *Proc. WOMBAT Workshop on Information Security Threats Data Collections And Sharing*, pp.58–66 (2008).
[12] Malécot, E.L. and Inoue, D.: The Carna Botnet Through The Lens of a Network Telescope, *Proc. 6th International Symposium on Foundations and Practice of Security* (*FPS'03*), pp.426–441 (2013).
[13] 笠間貴弘，島村隼平，井上大介：パッシブ観測とアクティブ観測を組み合わせた組込み機器の攻撃活動状況の把握，電子情報通信学会論文誌，Vol.J99-A, No.2, pp.94–105 (2016).
[14] 笠間貴弘，井上大介：アクティブ観測結果に基づく攻撃元機器の分類手法，電子情報通信学会技術研究報告 = IEICE Technical Report：信学技報，Vol.116, No.328, pp.37–42 (2016).
[15] Moore, D., Shannon, C., Voelker, G.M. and Savage, S.: Network Telescopes: Technical Report, Cooperative Association for Internet Data Analysis (CAIDA) (2004).
[16] Bailey, M., Cooke, E. and Nazario, F.J.J.: The internet motion sensor: A distributed blackhole monitoring system, *Proc. 12th Annual Network and Distributed System Security Symposium* (*NDSS'05*) (2005).
[17] Kálnai, P. and Malik, M.: New Linux/Rakos threat: Devices and servers under SSH scan, available from ⟨https://www.welivesecurity.com/2016/12/20/new-linuxrakos-threat-devices-servers-ssh-scan/⟩ (accessed 2017-05-31).
[18] 警察庁：「Mirai」ボットの亜種等からの感染活動と見られるアクセスの急増について，入手先 ⟨https://www.npa.go.jp/cyberpolice/important/2017/19824.html⟩ （参照 2017-05-31）.
[19] Bambenek, J.: UPDATED x1: Mirai Scanning for Port 6789 Looking for New Victims / Now hitting tcp/23231, available from ⟨https://isc.sans.edu/forums/diary/UPDATED+x1+Mirai+Scanning+for+Port+6789+Looking+for+New+Victims+Now+hitting+tcp23231/21833/⟩ (accessed 2017-05-31).
[20] Bruneau, G.: Request for Packets and Logs - TCP 5358, available from ⟨https://isc.sans.edu/forums/diary/Request+for+Packets+and+Logs+TCP+5358/21997/⟩ (accessed 2017-05-31).
[21] Ullrich, J.B.: TR-069 NewNTPServer Exploits: What we know so far, available from ⟨https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/⟩ (accessed 2017-05-31).
[22] Fengpei, L.: New Threat Report: A new IoT Botnet is Spreading over HTTP 81 on a Large Scale, available from ⟨http://blog.netlab.360.com/a-new-threat-an-iot-botnet-scanning-internet-on-port-81-en/⟩ (accessed 2017-05-31).
[23] Kim, P.: Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server, available from ⟨https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html⟩ (accessed 2017-05-31).
[24] MAXMIND: GeoIP Databases & Services: Industry Leading IP Intelligence, available from ⟨https://www.maxmind.com/en/geoip2-services-and-databases⟩ (accessed 2017-05-31).
[25] Durumeric, Z., Adrian, D., Mirian, A., Bailey, M. and Halderman, J.A.: A Search Engine Backed by Internet-Wide Scanning, *Proc. 22nd ACM Conference on Computer and Communications Security* (*CCS'15*), pp.542–553 (2015).
[26] Shodan: The search engine for the Internet of Things, available from ⟨https://www.shodan.io/⟩ (accessed 2017-05-31).
[27] The Shadowserver Foundation: Shadowserver Foundation - Main - HomePage, available from ⟨https://www.shadowserver.org/wiki/⟩ (accessed 2017-05-31).
[28] Cilibrasi, R. and Vitanyi, P.M.: Clustering by Compression, *IEEE Transactions on Information Theory*, Vol.51, No.4, pp.1523–1545 (2005).
[29] Li, M., Chen, X., Li, X., Ma, B. and Vitanyi, P.M.: The Similarity Metric, *IEEE Trans. Information Theory*, Vol.50, No.12, pp.3250–3264 (2004).
[30] Lyon, G.: Nmap: The Network Mapper — Free Security Scannere, available from ⟨https://www.shadowserver.org/wiki/⟩ (accessed 2017-05-31).
[31] Moore, H.: GitHub:scan-tools/banner-plus.nse at master, available from ⟨https://nmap.org/⟩ (accessed 2017-05-31).
[32] julian@bzip.org: bzip2, available from ⟨http://www.bzip.org/⟩ (accessed 2017-05-31).
[33] SciPy developers: SciPy.org, available from ⟨https://www.scipy.org/⟩ (accessed 2017-05-31).
[34] Lindqvist, U. and Neumann, P.G.: The future of the internet of things, *Comm. ACM*, Vol.60, No.2, pp.26–30 (2017).
[35] Sadeghi, A.-R.S., Wachsmann, C. and Waidner, M.: Security and privacy challenges in industrial internet of things, *Proc. 52nd Annual Design Automation Conference*, pp.1–6 (2015).
[36] Shannon, C. and Moore, D.: The spread of the witty worm, *IEEE Security & Privacy*, Vol.2, No.4, pp.46–50 (2004).
[37] Eto, M., Inoue, D., Song, J., Nakazato, J., Ohtaka, K. and Nakao, K.: Nicter: A large-scale network incident analysis system: Case studies for understanding threat landscape, *Proc. 1st Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, pp.37–45, ACM (2011).

[38] Durumeric, Z., Wustrow, E. and Halderman, J.A.: ZMap: Fast Internet-Wide Scanning and its Security Applications, *Proc. 22nd USENIX Security Symposium*, pp.605–620 (2013).
[39] micheloosterhof: Cowrie SSH/Telnet Honeypot, available from ⟨https://github.com/micheloosterhof/cowrie⟩ (accessed 2017-05-31).
[40] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C.: IoTPOT: Analysing the Rise of IoT Compromises, *Proc. 9th USENIX Workshop on Offensive Technologies* (*WOOT'15*) (2015).

笠間 貴弘 （正会員）

2014 年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）．2011 年情報通信研究機構に入所．現在はサイバーセキュリティ研究所サイバーセキュリティ研究室主任研究員として，マルウェア解析やネットワーク攻撃観測・分析等サイバーセキュリティの研究開発に従事．

井上 大介 （正会員）

2003 年横浜国立大学大学院工学研究科博士課程後期修了．2003 年通信総合研究所（現，情報通信研究機構）に入所．2006 年よりインシデント分析センター NICTER の研究開発に従事．現在，情報通信研究機構サイバーセキュリティ研究所サイバーセキュリティ研究室室長．2002 年暗号と情報セキュリティシンポジウム論文賞，2009 年科学技術分野の文部科学大臣表彰（科学技術賞），2013 年グッドデザイン賞，2014 年 Asia–Pacific Information Security Leadership Achievements 等を受賞．