マルチモーダル分析による組込みシステムからの攻撃活動状況の把握

笠間 貴弘† 島村 隼平‡ 井上 大介†

† 情報通信研究機構 184-8795 東京都小金井市貫井北町 4-2-1
{kasama, dai}@nict.go.jp

‡ 株式会社クルウィット 181-0013 東京都三鷹市下連雀 3-34-8 三鷹ハイデンス 509 号
shimamura@clwit.co.jp

あらまし ブロードバンドルータやDVRなどインターネットに接続された組込みシステムのマルウェア感染事例が複数報告され，新たな攻撃対象として注目されている．我々が行っているダークネット観測でも通常のWindowsマシンとは異なる組込みシステムと推測されるホストからのスキャン活動が観測されているが，ダークネット観測では到達するパケットに対して応答を返答しないため正確に送信元のシステムを判定するのは困難である．一方，能動的なクローリングによってインターネットに接続された組込みシステムを探索している組織・プロジェクトも存在する．そこで本稿では，我々のダークネット観測結果とそれらの能動的な観測情報を組み合わせたマルチモーダル分析を行うことで，組込みシステムからの攻撃活動状況を分析する．

Multimodal Analysis for Understanding Attack Activities of Embedded Devices

Takahiro KASAMA† Jumpei SHIMAMURA‡ Daisuke INOUE†

† National Institute of Information and Communications Technology.
4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, JAPAN
{kasama, dai}@nict.go.jp
‡ clwit, Inc. 3-34-8-509, Shimo-Renjaku, Mitaka, Tokyo 181-0013, JAPAN
shimamura@clwit.co.jp

Abstract Many security incidents that embedded devices such as broadband routers and digital video recorders are infected with malware have been reported. Now, those embedded devices are very attractive attacking targets for attackers. There are many packets which seem to be sent by embedded devices arrived at darknet. However, in darknet monitoring, since a blackhole sensor does not respond at all to incoming packets, it is hard to distinguish whether a source host is an embedded device or not. On the other hand, there are some research projects which conduct network scanning over the Internet for searching Internet-connected embedded devices. In this paper, we conduct a multimodal analysis which combines the above active scanning result with the passive (darknet) monitoring result for understanding attack activities of embedded devices.

1 はじめに

ブロードバンドルータをはじめとして，デジタルビデオレコーダ（DVR）のような AV 機器や家電製品，自動販売機に至るまで，多くの組込みシステムがインターネットに繋がる状況になっている．こうした背景から，組込みシステムが攻撃者にとっての魅力的な攻撃対象として認識されるようになり，実際多くの攻撃事例やマルウェア感染事例が報告されている．例えば，2010 年 2 月には，“Chuck Norris”[1][2]と呼ばれるブロードバンドルータに感染するボットネットの存在がチェコの研究者によって報告された．Chuck Norris は工場出荷時に設定されたデフォルトの ID とパスワードを用いてルータに感染したのち，脆弱性を利用したりネットワーク共有に対する辞書攻撃を行ったりすることで Windows マシンへ感染を広める機能を有していた．その他にも 2012 年には全世界で約 42 万台ものルータをはじめとする組込みシステムに感染した Carna ボットネット[3]が現れるなど，組込みシステムに対する攻撃が大きな脅威となっている．特に，上記のようなワームタイプのマルウェアの存在は，かつての Windows マシンにおける大規模感染ワームと同様に大きな被害につながる危険性が高いため，それらの感染拡大の兆候を注意深く観測・分析することが重要となる．

ワームタイプのマルウェアであれば，能動的に次の感染対象を探索するためのスキャン活動を行うため，ダークネット観測でその挙動を観測できる可能性がある．ダークネットとは，インターネット上で到達可能かつ未使用の IP アドレス空間のことを指し，そこに到達するパケットを観測・分析することで，マルウェアによるスキャン活動をはじめとした多くの不正活動の把握が可能となる．我々がインシデント分析センター NICTER[4][5]で観測している約 24 万 IP アドレスのダークネットにおいても，近年，TTL（Time to live）の値や送信元ポート番号といった情報から通常の Windows マシン以外から送信されたと推測されるパケットが多く観測されている．しかしながら，ダークネット観測では到達するパケットに対して応答を返答しないため，ダークネットに届くパケット情報のみで正確に送信元ホストが組込みシステムであるか否かを判断するのは困難である．一方，Shodan[6]のように，能動的にインターネット空間を探索し，インターネットに接続された組込みシステムを探索しているプロジェクトが存在する．能動的なクローリングを行うことによって，実際のホストのポート待ち受け状況が把握できることに加えて，Telnet（23/TCP）や HTTP（80/TCP）でアクセスした際の応答（バナー情報）を得ることができるため，ダークネット観測よりも精度良く送信元ホストの判断が可能である．

そこで本稿では，我々のダークネット観測結果と Shodan で検索可能な能動的な観測情報を突合することで，組込みシステムからの攻撃活動状況を分析する．

論文の構成は以下の通りである．まず，2 章において，過去の組込みシステムに対する攻撃事例を紹介する．その後，3 章でダークネットにおける攻撃観測データを示し，4 章で Shodan における観測データを示す．5 章では，それら二つの観測データを突合し，両者で観測された攻撃ホストに対して更なる分析を行う．最後に 6 章で考察とまとめを行う．

2 組込みシステムへの攻撃事例

本章では，実際に報告されている組込みシステムに対する攻撃事例について述べる．

組込みシステムに対する攻撃事例としては，設定や管理の不備を突いたケースと，脆弱性を悪用したケースが挙げられる．前者の場合，Telnet や Web の管理ページの ID やパスワードがデフォルト設定のまま運用されているケースが典型的な例となる．例えば，2010 年 2 月に報告された Chuck Norris と呼ばれるマルウェアは，Telnet スキャンを行い，応答があったホストに対して辞書攻撃を行うことでデフォルト設定のままの DSL モデムやルータに感染を拡げた．また，2012 年には匿名の人物が，インターネット上で安易な ID とパスワードでアクセス可能なルータ

等に対して感染を拡げる Carna ボットを作成し，計 42 万台もの組込みシステムに感染させ，インターネットの IPv4 空間全てをスキャンした結果を公開した．これらの事例は数多くの組込みシステムがインターネットからアクセス可能であり，かつ脆弱な ID とパスワードを利用していることで容易に攻撃者に侵入されうることを示している．

一方，脆弱性を悪用して組込みシステムを攻撃した事例も複数報告されている．2014 年 1 月には Synology 社製の NAS に攻撃者が任意のコードを実行可能となるアクセス制御不備の脆弱性が報告され，実際に当該脆弱性を使用した攻撃が観測される事例が報告されている[7]．同じく 2014 年 1 月に，Cisco，Linksys，Netgear などのルータにドキュメント等に記載されていない 32764/TCP で稼働するテストインタフェースが存在し，攻撃者はこのポートに対して特定のデータを送信することで任意のコマンドを実行可能であることが報告された[8][9]．その他にも Linksys のルータに存在する CGI の脆弱性を悪用して感染を拡げるマルウェア（The Moon）が報告され[10]，ビル管理システムで用いられるシステムに脆弱性が報告され当該システムを探索する活動が観測されるなど[11]，組込みシステムに対する攻撃活動が非常に活発に行われている．

3 ダークネット観測状況

2 章で示したとおり，組込みシステムが攻撃対象となり，実際にマルウェアに感染する事例が確認されているが，特にその中でも Carna ボットネットのようにマルウェアが能動的に次の感染対象を探索し感染を拡げていくワームタイプのマルウェアの存在は，かつての Sasser[12]や Conficker[13]，Morto[14]のように，大規模感染につながる可能性が高く，それらの感染拡大の兆候を注意深く観測・分析する必要がある．ワームタイプのマルウェアは，システムへの侵入後にインターネット上に対して広範囲なスキャンを行うことで次の攻撃対象となるシステムを探索するケースが多いため，特定のサービスに脆弱性が発見され，その脆弱性を悪用するワームタイプのマルウェアが現れた場合には，ダークネットにおいて当該サービスの稼働するポートに対するスキャン活動が急増する事例が多く報告されている[15]．

そこで，2 章で述べた各攻撃事例に関連したポートに対するダークネットの観測結果を図 1 から図 4に示す．各図では，2014 年 1 月から 7 月までの各宛先ポートに対する日毎の SYN パケット数（47808/UDP については UDP パケット）およびそれらのユニークホスト数（送信元ホストを IP アドレスでカウント）の推移を示している．

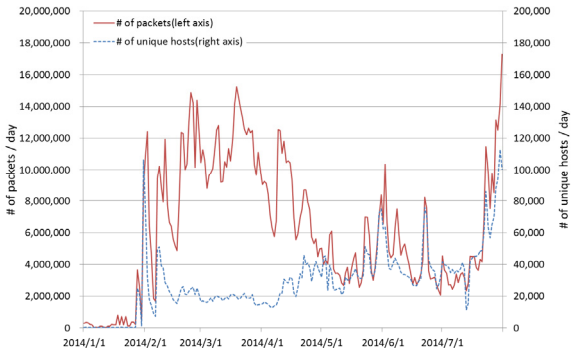

図 1 23/TCP の観測結果

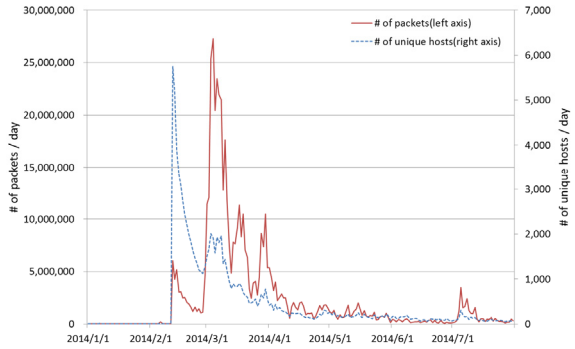

図 2 5000/TCP の観測結果

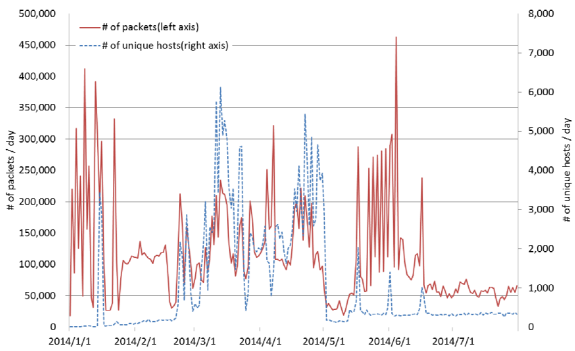

図 3 32764/TCP の観測結果

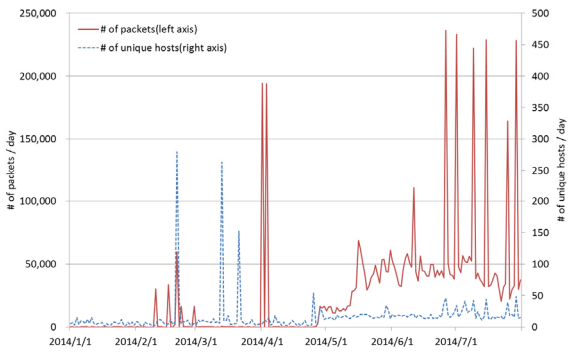

図 4　47808/UDP の観測結果

図 1を見ると, 2014 年 2 月直前から 23/TCP に対するパケット数とユニークホスト数が急激に増加している様子がわかる. また, その後一定数で推移していた値が 7 月中旬を境にまた顕著な増加傾向を示しており, 1 日に 10 万ホスト以上からのパケットを観測していることから, 何か大規模な感染活動が行われている可能性が高い. また, 図 2を見ると, こちらも 2 月 12 日から 5000/TCP に対する急激なピークを観測している. 2 章で述べた脆弱性の報告が 1 月であることから, その影響で攻撃活動が活発化した可能性がある. しかし, その後徐々に減少傾向を示し, 現状ではピーク時の 10 分の 1 程度の値で推移している. 図 3を見ると, 32764/TCP に対するパケット数が年明けから乱高下を繰り返している. 2013 年 12 月末までは当該ポートに対する通信はほぼ観測されていないことから, こちらも脆弱性の報告が契機となって攻撃活動が盛んになっていると考えられる. 図 4を見ると, 47808/UDP については 2 月中旬から複数回のピークが見られたのちに, 5 月以降は一定数で推移している.

表 1 に上記の観測期間において, 各宛先ポートに対してもっとも多くのユニークホスト数が観測された日のユニークホスト数(IP アドレス数)と送信元ホストの国情報の統計, それらのホストからの通信をパッシブ OS フィンガープリンティングツールである p0f[16]にかけた結果推定された OS 種類の統計を示す. なお, 47808/UDP に関しては, p0f では UDP パケットから OS 推定を行うシグネチャが存在しないため, OS 種類の統計は含まれない. また, 同一ホストから複数パケットが観測されている場合, p0f はそれぞれのパケットについて異なる OS 推定結果を出力するケースがあるが, 表 1 の OS 種別の統計ではその点は考慮せず単純に OS 種別毎に当該 OS と推定された IP アドレス数を示している.

表 1 を見ると, 23/TCP, 5000/TCP, 32764/TCP においては, それぞれ送信元国として中国が支配的であることがわかる. 一方, 47808/UDP については送信元国がメキシコやブラジル, アルゼンチンのような南米の国に偏っており, 他のポートとは攻撃元ホストの分布に明らかな偏りが存在するが要因は明らかではない. また, 23/TCP と 5000/TCP については p0f の判定結果を見てもほぼ全てが Linux 系 OS と判定されており, Windows マシンとは異なるホストからスキャンが行われていることが推測される. 32764/TCP についても, OS の推定結果は Linux 系 OS が上位だが, 他のポート番号とは異なり 9 割近くのホストが p0f のシグネチャにマッチせず, OS の判定ができていない点が異なる.

表 1　ダークネット観測結果の統計情報

port:23 (2014/07/30)		port:5000 (2014/02/12)		port:32764 (2014/03/13)		port:47808 (2014/02/20)	
IPアドレス数	112,993	IPアドレス数	5,748	IPアドレス数	6,116	IPアドレス数	280
国 Top 5		**国 Top 5**		**国 Top 5**		**国 Top 5**	
中国	53,207	中国	4,121	中国	2,903	メキシコ	57
インド	9,603	コロンビア	207	韓国	708	ブラジル	46
マレーシア	4,724	インド	141	アメリカ	276	アルゼンチン	41
ロシア	3,253	アメリカ	120	ケニヤ	269	スペイン	36
タイ	2,929	ブラジル	87	インド	265	チリ	17
(日本)	50	(日本)	4	(日本)	18	(日本)	2
OS Top 5		**OS Top 5**		**OS Top 5**		**OS Top 5**	
Linux 2.4.x	85,000	Linux 2.4.x	3,791	Linux 2.2.x - 3.x (barebone)	315	-	-
Linux 2.2.x - 3.x	45,777	Linux 2.2.x - 3.x	2,788	Linux 2.4.x	119	-	-
Linux 2.2.x - 3.x (no timestamp)	5,493	Linux 2.4.x - 2.6.x	314	Linux 2.2.x - 3.x	80	-	-
Linux 3.x	2,416	Linux 2.2.x - 3.x (no timestamp)	31	Linux 2.6.x	37	-	-
Linux 2.4.x - 2.6.x	1,252	Linux 2.6.x	30	Linux 2.2.x - 3.x (no timestamp)	8	-	-

4　検索エンジン Shodan

Shodan は 2009 年に John Matherly 氏によって開発された検索エンジンである．Shodan では能動的なクローリングによって，Web サーバだけに限らずインターネットに接続されたサーバ機能を有した機器を探索しており，それらの機器にアクセスした際に送られる応答メッセージ（バナー情報）をインデックス化して検索可能にしている．こうしたバナー情報（図 5）には製品名やバージョン情報をはじめとする機器やサービスの情報が含まれている場合があり，機器によってはデフォルト設定のログイン ID とパスワードの情報をインターネットで容易に見つけることができるため，適切な設定や管理が行われていない機器には攻撃者に侵入されてしまう危険性が存在する．

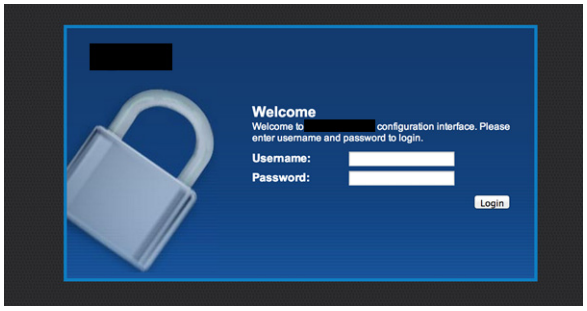

図 5　バナー情報の例（Web インターフェース）

表 2 に 3 章でダークネット観測結果を示した各ポート番号についての Shodan での検索結果を示す．表 2 では，総 IP アドレス数，国単位での上位 5 か国（＋日本）の統計情報のほか，組織，OS，製品単位での統計情報を示している．なお，総 IP アドレス数については過去全てのクローリング結果が含まれているため，現時点でアクセス可能な IP アドレス数を示しているわけではない．また，その他の統計情報についても，あくまでも Shodan 側で識別できたもののみの統計である．

表 2 の国情報の統計について，表 1 で示したダークネット観測結果と比較すると，23/TCP に関しては中国が共に支配的となっているが，それ以外については傾向は類似していないことがわかる．特に，5000/TCP および 47808/TCP では上位 5 か国全てが異なる国で構成されているなど，当該ポートにスキャンを行っているホストと当該ポートでアクセス可能なホストの分布傾向には関連性は低いと考えられる．一方，OS や製品情報については，そもそも全体の IP アドレス数と比較して識別されている数が少なく，多くのホストについては OS や製品に関する情報を得られていない．なお，識別できたものの OS の統計では，23/TCP と 5000/TCP についてはダークネット観測と同様に Linux OS が支配的である．一方，32764/TCP については識別できた OS の中

表 2　各ポート番号での Shodan 検索結果

port:23		port:5000		port:32764		port:47808	
IPアドレス数	64,421,247	IPアドレス数	1,336,485	IPアドレス数	30,585	IPアドレス数	14,741
国 Top 5		**国 Top 5**		**国 Top 5**		**国 Top 5**	
中国	26,927,950	韓国	275,896	アメリカ	11,200	アメリカ	9,211
アメリカ	3,615,584	アメリカ	168,962	中国	3,403	カナダ	2,477
韓国	3,544,277	ドイツ	127,749	イギリス	3,054	スペイン	296
ブラジル	2,069,736	フランス	86,909	イタリア	2,728	オーストラリア	268
ベトナム	1,900,906	カナダ	51,778	ブルガリア	911	フィンランド	244
（日本）	282,493	（日本）	11,901	（日本）	336	（日本）	47
組織 Top 5		**組織 Top 5**		**組織 Top 5**		**組織 Top 5**	
China Telecom Guangdong	3,054,334	Korea Telecom	244,373	Rethem Hosting LLC	4,095	AT&T Internet Services	982
China Telecom FUJIAN	1,603,983	Deutsche Telekom AG	60,784	Highland Community College	1,992	Comcast Business Communications	590
China Unicom Henan	1,567,383	Comcast Cable	53,949	Telecom Italia	1,631	Comcast Cable	336
China Telecom Jiangsu	1,266,086	Orange	37,879	America Online	1,286	Time Warner Cable	284
Korea Telecom	1,165,007	Rogers Cable	36,328	China Telecom JIANGXI	1,080	Shaw Communications	223
OS Top 5		**OS Top 5**		**OS Top 5**		**OS Top 5**	
Linux 2.6.x	254,128	Linux 2.6.x	73,713	Windows XP	234	-	-
Windows XP	76,856	Linux 3.x	25,106	Linux 2.6.x	51	-	-
Windows 7 or 8	27,970	Windows XP	2,848	Linux 2.4.x	45	-	-
Linux 2.4.x	25,523	Windows 7 or 8	2,497	Windows 7 or 8	17	-	-
Linux 3.x	16,711	Linux 2.4.x	1,775	Linux 3.x	13	-	-
製品 Top 5		**製品 Top 5**		**製品 Top 5**		**製品 Top 5**	
Cisco router telnetd	567,460	Apache httpd	626,556	AIM or ICQ server	769	Nagios NSCA	123
Check Point Firewall-1 telnetd	173,819	Ncat http proxy	21,915	OpenSSH	279	-	-
bnetd open source Blizzard Battlenet server	148,553	Microsoft IIS httpd	11,156	VNC	94	-	-
Open SSH	24,615	nginx	9,091	Microsoft Exchange smtpd	31	-	-
Cisco catalyst switch telnetd	21,154	mini_httpd	8,637	Microsoft ftpd	22	-	-

では Windows XP が 1 位となっており，ダークネット観測結果との差異が見られる．製品の統計情報を見ると，23/TCP では Cisco のルータ等の組み込み機器と見られる製品が上位になっており，5000/TCP では Apache httpd が 1 位になっているなど，2 章で示した攻撃事例に関連していると想定される製品が上位になっている．一方，32764/TCP と 47808/UDP では，識別できた製品情報の中では，ICQ（インスタントメッセンジャーソフト）や Nagios（各種サービス・リソースの監視用ソフト）が 1 位となっており，攻撃事例に対応した製品情報は得られなかった．

5　マルチモーダル分析

本章では，3 章のダークネット観測で観測された各宛先ポートに対する送信元 IP アドレスについて，4 章で示した Shodan による能動的なクローリングによって観測されているか否かを調べ，その詳細について分析を行う．

まず，各宛先ポートに対してダークネット観測期間中にユニークホスト数がピークを示している日について，観測された IP アドレス群が Shodan のデータベースに存在するか検索を行った結果を図 6に示す．なお，検索の際は，2014 年以降のデータのみに絞り，Shodan のクローリング結果に含まれるポート開放していたポート番号については条件指定していない．

図 6を見ると，各 IP アドレスリストにおいて 66%～88%の IP アドレスが Shodan のデータベースに存在している，つまり，各宛先ポート番号について，ダークネットに対してスキャンを行っているホストの半数以上は Shodan が観測対象としているポート番号のいずれかでアクセス可能であることがわかる．

また，表 3 に図 6に示した Shodan リストとマッチングできた IP アドレス群について国，宛先ポート番号，OS，製品の統計情報を示す．

表 3 を見ると，送信元国については図 5 のマッチング結果を見てもわかる通り，ダークネットで観測されたホストの大半が同様に Shodan でも

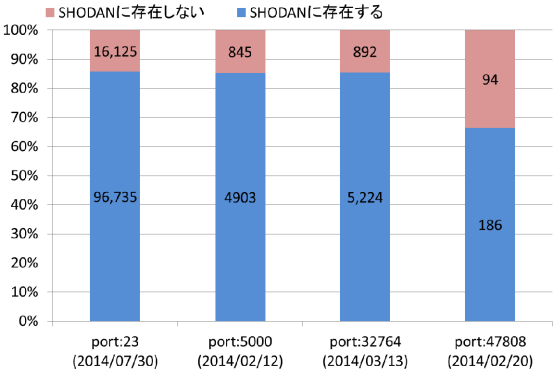

図 6　Shodan でのマッチング結果

表 3　Shodan データベースとマッチングできたホスト群の詳細情報

port:23 (2014/07/30)		port:5000 (2014/02/20)		port:32764 (2014/03/13)		port:47808 (2014/02/20)	
IPアドレス数	96,735	IPアドレス数	4,903	IPアドレス数	5,224	IPアドレス数	186
国 Top 5		**国 Top 5**		**国 Top 5**		**国 Top 5**	
中国	45,794	中国	3,505	中国	2,425	メキシコ	41
インド	9,337	コロンビア	191	韓国	732	アルゼンチン	36
マレーシア	4,662	インド	144	インド	263	ブラジル	34
タイ	2,911	アメリカ	105	アメリカ	260	スペイン	21
ロシア	2,845	ブラジル	83	ケニヤ	258	チリ	12
（日本）	50	（日本）	4	（日本）	18	（日本）	0
宛先ポート番号 Top 5		**宛先ポート番号 Top 5**		**宛先ポート番号 Top 5**		**宛先ポート番号 Top 5**	
23	57,831	23	3,959	23	4,424	80	81
80	51,912	80	2,127	80	2,164	1900	59
1,900	36,476	21	1,228	21	1,255	161	40
21	21,494	1900	977	1,900	1,090	23	34
161	11,184	443	331	443	416	8080	29
		(5000)	6	(32764)	5	(47808)	0
OS Top 5		**OS Top 5**		**OS Top 5**		**OS Top 5**	
(undef)	96,678	(undef)	4,898	(undef)	2,220	(undef)	186
Linux 2.6.x	8,516	Linux 2.6.x	477	Linux 2.6.x	106	Linux 2.6.x	11
Linux 3.x	671	Linux 3.x	15	Linux 3.x	29	Linux 2.4 - 2.6	4
Linux 2.4 - 2.6	534	Windows 7 or 8	13	Windows XP	29	Windows 7 or 8	2
Windows 7 or 8	207	Linux 2.4 - 2.6	8	Windows 7 or 8	19	Linux 3.x	1
製品 Top 5		**製品 Top 5**		**製品 Top 5**		**製品 Top 5**	
micro_httpd	15,759	Mini web server	503	Mini web server	372	Allegro RomPager	44
Dropbear sshd	10,674	Dropbear sshd	392	Dropbear sshd	350	Dropbear sshd	9
Allegro RomPager	10,344	Boa HTTPd	143	GoAhrad-Webs httpd	321	Apache httpd	8
D-Link DLS-2750U ftp firmward update	7,378	micro_httpd	103	Boa HTTPD	147	Netgear broadband router or ZyXel VoIP adapter ftpd	7
Mini web server	3,974	Allegro RomPager	60	bftpd	91	micro_httpd	6

観測されているため，ダークネット観測結果の傾向と類似している．また，各 IP アドレスに対する Shodan によるバナー情報に基づく製品の判定結果を見ると，“Mini web Server”，“Dropbear sshd”，“Allegro RomPager”，“GoAhead-Webs httpd”，“micro_httpd”といった名前が上位に入っていることがわかる．これらはどれもルータ等の組込みシステムに用いられることの多い軽量な SSH サーバや Web サーバ等のソフトウェア[17][18][19][20][21]であることから，これらのホストの多くは組込みシステムであり，それら組込みシステムがダークネットに対してスキャン活動を行っていると考えられる．さらに，Shodan の OS 判定結果が大半のホストについて不明（undef）となっている点も，それらのホストが組込みシステムであるため，通常の Linux 系 OS のシグネチャ等で判定できなかった可能性が考えられる．

しかしながら，5000/TCP，32764/TCP，47808/UDP の IP アドレス群に対しては，Shodan の観測でアクセス可能であったポート番号として 23/TCP（Telnet），80/TCP（HTTP），1900/UDP（UPnP），21/TCP（FTP）といったサービスが多数を占めており，それぞれがダークネットに対してスキャンを行っていた宛先ポートに関しては，アクセス可能なホストは殆ど存在していない．この結果から，上記の 3 つのポート番号に関しては，今のところ侵入時と同じ方法で感染を拡げるようなワームタイプのマルウェアの活動は行われていないと考えられる．また，実際には多くのホストが 23/TCP でアクセスが可能な状態になっていることから，Telnet の設定不備を突くなど，別の方法でマルウェアに感染し，攻撃者によってスキャン活動に利用されている可能性が高い．

一方，23/TCP に対してスキャンを行っているホストについては，同様に 23/TCP でポート待ち受けを行っているホストが多いことから，23/TCP（Telnet）を悪用して感染を拡げるワームタイプのマルウェアが活動している可能性が高いと推測できる．また，Shodan とマッチングできた各ホストのダークネットで観測された挙動を詳細に調べたところ，一部のホストが 23/TCP 宛てのスキャン活動に加えて 10073/TCP を宛先ポートとするスキャン活動を行っている様子が観測された．上記の挙動を示すあるホストの挙動を図 7に示すロジックで可視化した画像を図 8に示す．図 8に示したホストは，同一 IP アドレス宛てに 1 分程度の間隔で 23/TCP と 10073/TCP 宛てにパケットを送信しており，最近このような 23/TCP と 10073/TCP を両方スキャンしてくるホストが多数観測されている．SANS の Internet Storm Center による攻撃観測データでも 10073/TCP に対する攻撃の増加傾向が観測されている[22]ことから，インターネット上で大規模なスキャン活動が行われている可能性がある．この 10073/TCP については，送信元ホストに対してアクセスを試みてもポート待ち受け状態にはなっておらずアクセスできないことから，実際に何のサービスが当該ポートで動作しており，どういった目的で組込みシステムと推測されるホストがスキャンを行っているのか現状では明確ではない．こうした未知のサービスに対するスキャン活動は新たな脆弱性を悪用しようとする兆候である可能性が高く，また今回はそのスキャンを行っているホストが組込みシステムであることからも，今後注意深くその動向を観測する必要があると考えられる．

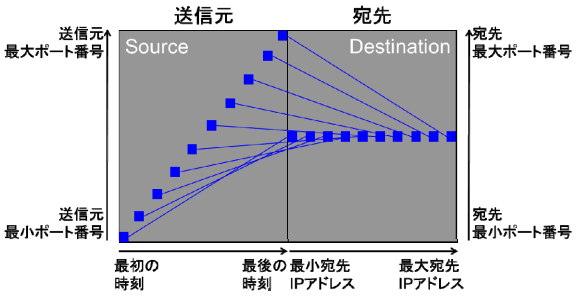

図 7　振る舞い分析の可視化方法

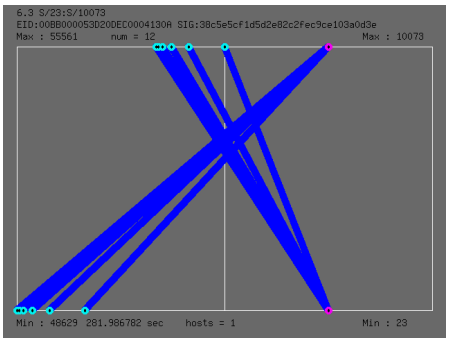

図 8　23/TCP と 10073/TCP に対してスキャンを行うホストの挙動

6 おわりに

本稿では，受動的な観測手法であるダークネット観測の結果と能動的な観測手法である Shodan によるクローリング結果を突合したマルチモーダル分析を行うことで，組込みシステムからの攻撃活動の分析を行った．二つの観測結果を組み合わせることで，組込みシステムへの攻撃に関連したポートに対するスキャン活動が実際に組込みシステム自身によって行われており，特に 23/TCP に関しては，スキャンを行っているホストの多くが 23/TCP でインターネットからアクセス可能な状態であることから，自ら感染を拡げるワームタイプのマルウェアが実際に活動している可能性が高いことが明らかになった．

参考文献

[1] P. Celeda, R. Krejci, J. Vykopal, M. Drasar, “Embedded Malware – An Analysis of the Chuck Norris Botnet,” In Proceedings of the 2010 European Conference on Computer Network Defense, pp. 3-10, October 2010.

[2] “Chuck Norris botnet karate-chops routers hard - Good Gear Guide by PC World Australia,” http://www.pcworld.idg.com.au/article/336938/chuck_norris_botnet_karate-chops_routers_hard/

[3] “Internet Census 2012 - Port scanning /0 using insecure embedded devices,” http://internetcensus2012.bitbucket.org/paper.html

[4] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, and K. Rikitake, “nicter: An Incident Analysis System using Correlation between Network Monitoring and Malware Analysis,” In Proceeding of the 1st Joint Workshop on Information Security, June 2006.

[5] “nicterWeb,” http://www.nicter.jp/nw_public/scripts/index.php#nicter

[6] “SHODAN - Computer Search Engine,” https://www.Shodan.io/

[7] “JVNVU#95919136: Synology DiskStation Manager にアクセス制御不備の脆弱性,” http://jvn.jp/vu/JVNVU95919136/

[8] E. Vanderbeken, “TCP-32764: some codes and notes about the backdoor listening on tcp-32764 in linksys WAG200G,” https://github.com/elvanderb/TCP-32764

[9] Cisco, “Undocumented Test Interface in Cisco Small Business Devices,” http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140110-sbd

[10] SANS ISC, “Linksys Worm "TheMoon" Summary: What we know so far,” https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633

[11] @police, “ビル管理システムに対する探索行為の検知について,” http://www.npa.go.jp/cyberpolice/detect/pdf/20140404.pdf

[12] Symantec, “W32.Sasser.Worm,” http://www.symantec.com/security_response/writeup.jsp?docid=2004-050116-1831-99

[13] Symantec, “W32.Downadup,” http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2008-112203-2408-99

[14] Symantec, “W32.Morto,” http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2011-082908-4116-99

[15] 中里純二，島村隼平，衛藤将史，井上大介，中尾康二，“nicter によるネットワーク観測および分析レポート ～ネットワークインシデントの前兆～,” 電子情報通信学会 信学技報, vol. 113, no. 95, ICSS2013-14, pp. 79-84, 2013 年 6 月.

[16] M. Zalewski, “p0f v3 (version 3.07b),” http://lcamtuf.coredump.cx/p0f3/

[17] “Dropbear SSH,” https://matt.ucc.asn.au/dropbear/dropbear.html

[18] “MiniWeb,” http://miniweb.sourceforge.net/

[19] “>Embedded Web Server Toolkits - Device Management | Allegro Software,” http://www.allegrosoft.com/embedded-web-server

[20] “GoAhead WebServer を使う,” http://www.ne.jp/asahi/it/life/it/windows/windows_network/goahead_webserver.html

[21] “micro_httpd - really small HTTP server,” http://www.acme.com/software/micro_httpd/

[22] “SANS Internet Storm Center,” https://isc.sans.edu/