ダークネットトラフィックの相関分析

深澤成孝[†1]　佐藤直[†1]

ダークネットでは，DDoS 攻撃、DNS アンプ攻撃などの大規模な攻撃を行うための事前活動や新しいマルウェアの出現によるスキャン活動などのトラフィックが観測される事例が数多く報告されている．また，近年，官公庁・政府機関・企業などを狙った標的型攻撃や新たな攻撃手法である水飲み場型攻撃などのサイバー攻撃は，今まで以上に高度化・巧妙化している．

本論文においては，日本における NICTER と世界規模の NORSE，二つのダークネット観測網のトラフィックデータの相関分析を行い，両者のダークネットトラフィックに相関関係があることがわかった．

Correlation Analysis of darknet traffic

HIDETAKA FUKAZAWA[†1]　NAOSHI SATO[†1]

In the darknet, abnormal packet traffic related with prior activity for performing DDoS attacks and DNS amp attack can be observed. Scanning activity by some new malware could be detected also on the darknet. So far many researchers have identified various types of attacks with the analyses of darknet traffic and delivered effective information of detecting an attack at an early stage. They are an offensive omen and an omen of large-scale infection. Especially in recent years，the cyber attacks have been sophisticated, and some of them are called APT (Advanced Persistence Threat) which targets government and related agencies and companies.

In this paper, we perform a correlation analysis of traffic data of two different darknet observation systems, NICTER and NORSE.　It was found that there is a correlation between the darknet traffic observed in these two systems.

1.　はじめに

インターネットは，個人，企業が生活や仕事を行っていく上で必要不可欠なものとなっている．今日では，インターネットの普及とともに，情報は紙媒体から電子媒体，アナログからデジタルへなどの移行が進み，個人情報，金融情報，国家の機密情報など多種多様な情報がインターネットと接続される環境に置かれている．一方，悪意のある利用者による攻撃がインターネットで後を絶たず, 近年では，一昔前までとは異なり，攻撃の精度はより高度化・巧妙化している．その代表的な攻撃として，官公庁・政府機関・企業などを狙った標的型攻撃[1]や水飲み場型攻撃[1]などが発生している．また，特定の機関や企業を狙った攻撃だけではなく，全世界のユーザをターゲットとした大規模な感染を狙ったマルウェアによる攻撃やソフトウェアの脆弱性を狙った攻撃なども行われている．

上記のような多様な攻撃が行われているインターネット空間において，マルウェアの発生，DDoS 攻撃などのセキュリティインシデントを検知する方法の一つとして，インターネット上で到達可能かつ未使用な IP アドレス空間であるダークネットに関する研究がある。ダークネットに届くトラフィックは，インターネット空間における数多くある攻撃の準備段階の一つであるとされ，多くの研究がなされている．

本研究においては、日本における NICTER と世界規模の NORSE で観測されるダークネット網のトラフィックデータを相関分析することにより、ダークネットトラフィックの特徴を見つけ出すことを目的とする．

2.　ダークネットの特徴

本章では，ダークネットの観測網及びダークネットでの観測状況について述べる．

2.1　ダークネットの観測網

日本での大規模なダークネット観測を行っている機関の一つに，情報通信研究機構（NICT）[2]がある．NICT では，インシデント分析センターNICTER[3]を使用してダークネット網の観測を行っている．NICTER では，日本で未使用の IP アドレス群である２１万アドレスからなるダークネット網を日々観測し，独自の解析システムで分析を行い，脅威が検知されれば，関係機関等への注意喚起を行っている．

図１．NICTER の全体像[4]

[†1] 情報セキュリティ大学院大学
Graduate School of Information Security INSTITUTE of INFORMATION SECURITY

次に，世界での大規模なダークネットの観測を行っている機関の一つに，米国セキュリティ会社の NORSE 社[5]がある．NORSE 社では，40 カ国以上，数百ヶ所のダークネットにハニーポットを仕掛け，収集される情報を分析している．その分析した情報を，2014 年 3 月 20 日から新しく改良した NORSE IPViking Live（国家間のサイバー攻撃を可視化したツール）を使用し，一般に公開している[6]. なお，公開されるデータは閲覧性などの理由で全体の一%程度.

図２．NORSE IPViking Live の画面[6]

その他に，大規模なダークネット観測網を設置し研究を行っている主な機関は以下のとおりある．

・PRACTICE：総務省の研究開発委託「国際連携によるサイバー攻撃予知技術の研究開発（PRACTICE）」によるダークネット観測プロジェクト[7]。

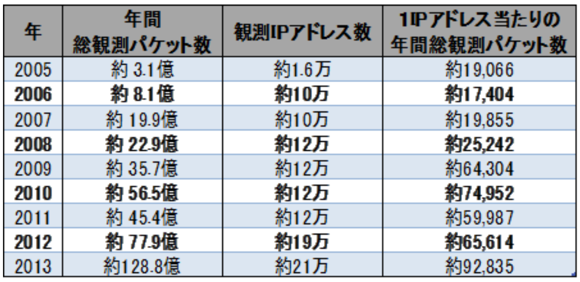
・Network Telescope：米国のカリフォルニア大学の CAIDA（Cooperative Association for Internet Data Analysis）によるダークネット観測プロジェクト。1600 万アドレス以上のダークネットを観測[8]。

・Internet Motion Sensor：米国のミシガン大学による 1700 万アドレス以上の大規模ダークネット観測プロジェクト[9]。

2.2 ダークネットでの観測状況

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な IP アドレス空間のことをいい，通常，未使用な IP アドレス空間に通信が届くことはほとんどないが，実際は，ダークネットの IP アドレス空間に対して，毎日多くのパケットが届いている．今までに NICTER で観測されたダークネットのトラフィック量は表 1 のとおりであり，ダークネットで観測されているデータは，毎年増加の一途を辿っていることがわかる．

表１　ダークネットトラフィック量[4]



年	年間 総観測パケット数	観測IPアドレス数	1IPアドレス当たりの 年間総観測パケット数
2005	約 3.1億	約1.6万	約19,066
2006	**約 8.1億**	**約10万**	**約17,404**
2007	約 19.9億	約10万	約19,855
2008	**約 22.9億**	**約12万**	**約25,242**
2009	約 35.7億	約12万	約64,304
2010	**約 56.5億**	**約12万**	**約74,952**
2011	約 45.4億	約12万	約59,987
2012	**約 77.9億**	**約19万**	**約65,614**
2013	約128.8億	約21万	約92,835

3. ダークネットの有用性

本章では，ダークネット観測から見えてきた攻撃の種類及び攻撃の予兆について述べる．

3.1 ダークネット観測から見えてきた攻撃の種類

ダークネットは，通常，ユーザが利用しない未使用の IP アドレス空間であるため，この空間でなんらかの大量の通信が観測された場合，何らかの攻撃が行われていると予想することができる. 2005 年から現在までにかけて, NICTER のダークネット網で観測を行ってきた結果，以下の４種類の攻撃予兆などが見えてきた．[4]

(1)マルウェアによるスキャン

・「ワーム側マルウェアの探索活動」・・マルウェアに感染したホストが次の感染先を探すためにネットワークのスキャン活動を行った際に観測される通信.

・「マルウェア感染の大局的傾向」・・マルウェア感染行動によって引き起こされる通信のパターンによって，新たなマルウェア発生の予兆が検知できる可能性.

・「感染爆発の前兆」・・マルウェアの振る舞いパターンによって，マルウェアの大規模感染の予兆が検知できる可能性.

(2)DDoS 攻撃の跳ね返り

・「送信元 IP アドレスが偽装された SYN Flood」・・backscatter 攻撃による跳ね返りが送信元 IP アドレスを偽装された第三者に送信されたことを検知.

・「被攻撃サーバからの応答（SYN-ACK）」・・偽装された IP アドレスからの SYN Flood 攻撃により, 攻撃先のサーバから返答される SYN-ACK を検知することで, SYN-Flood 攻撃が行われていることを検知.

・「DDoS」攻撃の早期検知・・DNS トラフィックが大量に検知されることにより，DDoS 攻撃が行われていることを検知.

(3)設定ミス

・「ネットワーク機器やサーバ機器などの設定ミス」・・システム構築時やネットワーク運用中の設定ミスによるパケットの検知.

(4)リフレクション攻撃の準備活動

・「DNS Open Resolver 探索」・・Open Resolver である DNS サーバを探し出し，DNS amp 攻撃を仕掛ける前の前兆を検知.

・「NTP 探索」・・NTP サーバを探し出し，DDoS 攻撃を仕掛ける前の前兆を検知.

3.2 ダークネット観測から見えてきた実際の攻撃予兆

NICTER のダークネット観測網で見えてきた実際の攻撃予兆の一例として, 2013 年 3 月 18 日に発生した「Spamhaus への DDoS 攻撃」がある．Spamhaus とは，スパム対策のサービスを全世界向けに行っている英国を拠点に活動する非

営利団体のことであり，多くのインターネットユーザのスパムメールなどをフィルタリングする支援などを行っている[10]．この DDoS 攻撃は最大で 300 Gbit/s の規模にも及ぶものであり，使われた手法が 3.1 で取り上げた「DNS amp 攻撃」である．

DNS amp 攻撃とは，DNS の名前解決の特性を突いた攻撃手法である．通常，DNS 通信は，要求と応答の二つから成り立っており，応答には要求と回答の二つが含まれている．そのため，DNS 通信は要求よりも応答の方がデータサイズが大きくなる特性があり，この特性を利用して図３の攻撃手法を用い DDoS 攻撃を行ったものである．この攻撃では，DNS 要求時のデータサイズが 26byte に対し，応答時のデータサイズは 821byte となり，約 32 倍の増幅であった．

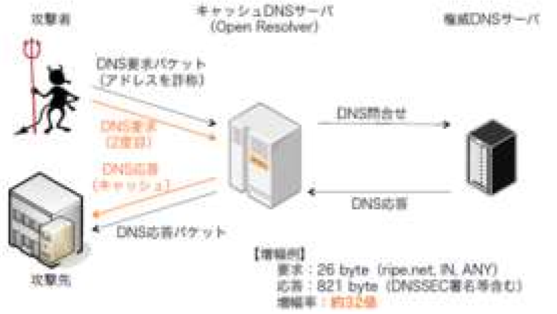


図３　DNS amp 攻撃の概要[4]

DNS amp 攻撃を行うにあたり，Open Resolver サーバが IP アドレス空間上のどこに設置されているかを確認する必要があるため，UDP/53 による Open Resolver の探索スキャンが事前に発生することになる．実際に，NICTER のダークネット観測網では，図４のとおり一時的に Spamhaus 攻撃日の前後に，UDP/53 による Open Resolver の探索スキャンが発生していた．

図４　パケット数（宛先 53/UDP）[4]

4.　ダークネット観測における関連研究

本章では，ダークネット観測における先行研究は幅広いが，ここでは本文の研究目的と関連する先行研究について述べる．

4.1　複数国ダークネット観測による攻撃の局地性分析 [11]

この研究では，総務省の研究開発委託「国際連携によるサイバー攻撃予知技術の研究開発（以下，PRACTICE)」を利用した研究であり，PRACTICE では，国際連携の一環として連携国に対してダークネットセンサを設置し，ダークネットトラフィックの観測・分析，サイバー攻撃情報の共有等を行っている．この研究では，４ヵ国のダークネットで観測される攻撃の傾向の比較を行い，特定国においてのみ観測されたり特定国からのみ届くなど局地性のある攻撃について分析を行っている．

その結果，実際に特定国から当該国に対してのみ観測される特徴的な攻撃が確認された．このような攻撃の情報を当該国に提供することで，各国の事情に合ったより効果的な対策を行うことができると期待される．

5.　ダークネットトラフィックの相関分析

今まで述べたことから、ダークネット網で観測されるトラフィックを解析することは，ライブネットにおける攻撃を事前に把握可能として有用性が高いことがいえる．

ついては本研究においては，日本の NICTER で観測されるダークネット網では，海外のダークネット網のトラフィックと分析を行った事例はないことから，日本の NICER と米国 NORSE 社の NORSE IPViking Live で観測されたトラフィックの相関分析を行う．

日本と世界規模で観測されているダークネット網のトラフィックデータを以下の基準を基に分析を行った．

（１）対象データ

日本　NICT：NICTER　Darknet 2014
　　　NONSTOP を利用してデータを収集
世界　NORSE：　NORSE IPViking Live（以下，NORSE と呼ぶ）．Wireshark を利用してデータを収集

（２）対象期間

2014 年 10 月 7 日～2014 年 11 月 4 日

（３）相関分析で使用する NICTER 及び NORSE での取得項目

NICTER・・観測時刻，攻撃元 IP アドレス・port・国
NORSE・・観測時刻，攻撃元 IP アドレス・port・国，攻撃先国

5.1　日別での検知数

（１）日別での検知数（一覧）

検知数を一覧にしたところ，表２のとおり NICTER 及び NORSE とも大量にダークネット網へのトラフィックデータを検知していることが判明した．

表 2　日別での検知数

日別	10/7	10/8	10/9	10/10	10/11	10/12	10/13
	火	水	木	金	土	日	月
nicter	1552569	1185526	1144846	1224944	1375643	1391719	1368824
norse	542652	556876	276048	307713	393366	654022	400155
日別	10/14	10/15	10/16	10/17	10/18	10/19	10/20
	火	水	木	金	土	日	月
nicter	1415645	1356924	1327984	1615894	1539433	1312528	1322649
norse	314961	270430	358454	450118	424121	309594	294667
日別	10/21	10/22	10/23	10/24	10/25	10/26	10/27
	火	水	木	金	土	日	月
nicter	2321514	1523457	1603808	1376530	1382970	1366670	1245863
norse	311864	329760	297670	309303	323381	304918	337368
日別	10/28	10/29	10/30	10/31	11/1	11/2	11/3
	火	水	木	金	土	日	月
nicter	1456719	1443864	1339162	1554444	1502135	1625611	1665051
norse	369938	389959	374841	446588	363129	385716	380809
日別	11/4						
	火						
nicter	1531991						
norse	383708						

（２）日別での検知数（グラフ）

次に，日別の検知数をグラフ化したところ，NICTER 及び NORSE とも日によって検知数に上限があることが判明した．また，NICTER では検知数が急激に増加している日でも，NORSE では一定の検知数の日であるなど特徴が現れていることから，検知数が多い日には何かしらの活動が行われている可能性が高い．

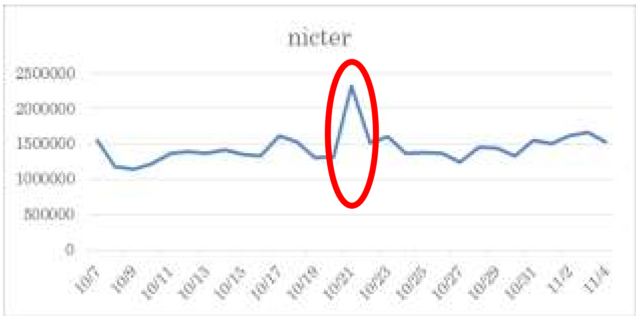


図 5　NICTER の日別検知数

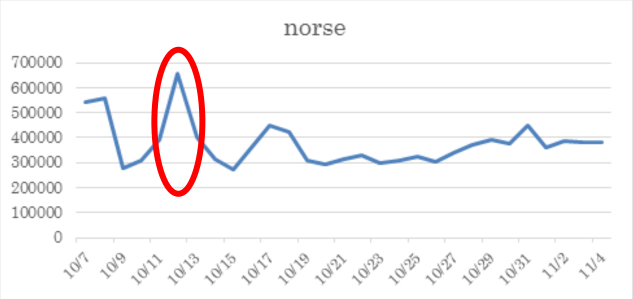


図 6　NORSE の日別検知数

次に，以下の項目について相関関係があるかどうかを検証する．これにより，日本と世界で観測されるダークネットトラフィックを分析することにより，世界規模，もしくは日本でのトラフィックの傾向を見出すことが可能となる．

・NICTER 及び NORSE で観測されるもの．
・NICTER で観測されるが NORSE では観測されないもの．
・NICTER で観測されないが NORSE で観測されるもの．

5.2　特定日の時間別での検知数

5.1 において，NICTER で急激にトラフィックが増加をした 10 月 21 日を対象に時間別に相関分析を行った．分析手法として，NICTER で検知数が多い IP アドレスを基準とし，NORSE で同様の IP アドレスが検知されていないかを確認した．

その結果，表 3 のとおり，検知した時間帯を黒色にしたところ，NICTER 及び NORSE の双方において，重複して観測された IP アドレスがあること，また，NICTER でしか観測されていない IP アドレスがあることが判明した．

表 3　10 月 21 日の IP アドレス別，時間別の検知数

nicter

	ipアドレス／時間	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	domain1	1704	1578	1668	1723	1595	1621	1753	1580	1653	1841	1763	1730	1744	1680	1821	1702	1699	1780	1711	1677	1747	1752	1750	1677
2	domain2	0	0	0	0	2383	0	3370	0	3242	0	3588	0	3229	0	3190	0	3511	3204	0	3283	3258	0	3275	0
3	domain3	0	0	0	0	0	0	0	0	0	0	0	0	8097	8695	7199	0	0	0	0	0	0	0	0	0
4	domain4	815	975	1683	2118	1236	920	903	850	836	876	901	919	903	878	922	930	838	846	840	874	920	859	857	849
5	domain5	0	0	0	0	0	0	0	0	0	0	0	0	7312	8688	7143	5	0	0	0	0	0	0	0	0
6	domain6	0	0	0	3120	5198	2220	1956	2925	2866	2449	1741	365	0	0	0	0	0	0	0	0	0	0	0	0
7	domain7	1458	1204	1098	1162	1066	1059	1095	1096	1195	1084	1078	1120	1118	1170	1129	1062	233	0	0	0	0	0	0	0
8	domain8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7983	9110	646	0	0
9	domain9	628	597	605	644	573	634	607	592	606	625	604	550	589	591	593	551	581	262	624	614	584	600	626	608
10	domain10	1	807	1029	1015	1011	234	874	964	976	1043	239	0	0	0	0	0	0	0	0	356	1140	1158	1069	373
11	domain11	0	0	0	0	0	0	0	0	0	0	0	4096	4096	0	0	0	0	0	0	0	0	0	4095	0
12	domain12	504	479	517	513	504	462	514	472	502	511	510	497	514	492	463	541	496	519	506	523	557	517	475	531
13	domain13	372	431	426	395	438	373	390	421	390	382	392	365	378	407	455	400	412	393	399	378	386	407	411	403
14	domain14	434	415	413	399	418	385	411	359	416	390	341	380	449	358	369	415	431	447	368	422	409	377	413	383
15	domain15	393	377	382	345	420	378	408	417	421	354	406	418	403	397	398	403	419	411	420	371	426	408	382	433
16	domain16	386	379	393	380	413	408	396	389	427	374	387	393	425	388	431	390	408	406	383	396	394	393	430	400
17	domain17	383	348	415	390	409	425	419	420	393	382	395	397	425	387	386	376	387	391	399	400	412	380	395	405
18	domain18	372	392	348	391	375	424	440	418	403	419	390	418	394	381	377	390	376	399	410	383	373	395	411	409
19	domain19	337	404	373	335	389	314	333	364	360	352	311	348	349	359	360	348	370	364	347	408	351	412	332	382
20	domain20	0	0	0	0	0	0	0	0	0	0	0	0	2688	2856	2937	0	0	0	0	0	0	0	0	0
21	domain21	0	0	0	0	0	0	0	0	0	0	0	0	2660	3088	2658	0	0	0	0	0	0	0	0	0
22	domain22	0	0	0	0	0	0	0	0	0	0	0	0	2480	3034	2798	0	0	0	0	0	0	0	0	0
23	domain23	0	0	0	0	0	0	0	0	0	0	0	0	4096	0	0	0	0	0	4096	0	0	0	0	0
24	domain24	4096	0	0	0	0	4096	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	domain25	0	0	0	0	0	0	0	0	0	640	608	640	608	640	640	608	640	640	608	640	608	640	32	0
26	domain26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8192	0	0	0	0	0	0	0
27	domain27	0	0	0	0	0	0	0	0	0	0	0	0	0	1025	1331	994	740	0	0	0	995	1305	937	859
28	domain28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7874
29	domain29	297	309	309	264	280	303	263	302	296	282	312	286	298	273	265	289	275	319	264	291	299	283	298	283
30	domain30	272	254	343	271	268	264	304	260	297	327	298	269	244	287	263	273	275	257	302	340	241	323	325	265
31	domain31	262	297	252	261	276	278	302	247	317	306	282	289	272	288	287	276	283	287	298	270	299	308	267	289
32	domain32	0	0	0	0	0	0	0	0	0	0	0	0	2610	2709	1124	0	0	0	0	0	0	0	0	0
33	domain33	46	0	188	284	249	244	247	235	219	259	261	228	284	259	259	253	257	255	231	428	425	432	436	429
34	domain34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6353	0	0	0	0	0	0	0	0
35	domain35	0	0	0	0	0	0	0	0	0	4093	0	0	0	0	0	0	0	0	0	0	0	0	0	2132
36	domain36	0	0	0	0	0	0	0	0	0	0	0	0	1984	2193	2031	0	0	0	0	0	0	0	0	0
37	domain37	0	0	0	0	0	0	0	0	0	0	0	0	1741	2096	2136	0	0	0	0	0	0	0	0	0
38	domain38	0	0	0	0	0	0	0	0	0	0	0	0	1847	2021	1882	0	0	0	0	0	0	0	0	0
39	domain39	232	261	210	245	230	190	197	233	220	257	233	221	222	230	217	238	241	234	232	199	237	224	223	247
40	domain40	0	0	0	0	0	0	0	0	0	0	0	4096	301	293	274	0	0	0	0	0	0	0	0	0
41	domain41	0	0	0	0	0	0	0	0	0	0	0	0	1528	1775	1627	0	0	0	0	0	0	0	0	0

norse

	ipアドレス／時間	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	domain1	132	220	250	135	200	147	107	105	119	96	192	280	123	130	109	118	193	271	118	202	155	116	233	202
2	domain2	39	365	23	99	40	291	44	66	79	50	122	38	96	35	87	57	84	127	97	113	78	57	172	44
3	domain3	0	0	0	0	0	0	0	0	0	0	0	0	31	286	107	40	0	0	0	0	0	0	0	0
4	domain4	48	116	178	168	180	89	71	54	70	52	102	119	49	87	40	66	103	136	69	108	84	46	100	122
5	domain5	0	0	0	0	0	0	0	0	0	0	0	0	44	269	129	43	0	0	0	0	0	0	0	0
6	domain6	0	0	0	13	291	177	25	33	28	32	113	81	0	0	0	0	0	0	0	0	0	0	0	0
7	domain7	11	82	110	7	84	40	15	13	13	11	62	110	10	34	9	14	25	0	0	0	0	0	0	0
8	domain8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	568	443	56	0	0
9	domain9	41	89	99	42	75	51	56	53	37	28	64	96	31	53	46	38	71	56	48	77	60	33	84	65
10	domain10	70	132	175	73	143	69	41	93	65	55	44	0	0	0	0	0	0	0	0	0	124	68	149	99
11	domain11	0	0	0	10	10	6	6	12	2	0	0	0	22	0	0	10	11	5	10	19	22	29	38	14
12	domain12	37	56	94	22	64	44	43	19	39	23	58	71	33	41	43	40	48	103	31	68	47	19	43	85
13	domain13	34	65	62	20	57	45	19	25	16	30	41	56	30	35	28	24	48	62	35	49	39	29	56	63
14	domain14	0	8	4	4	4	8	6	0	0	6	8	7	4	0	2	7	8	10	4	3	12	0	9	4
15	domain15	32	57	54	30	53	34	25	32	20	21	48	71	29	31	29	30	64	78	32	56	35	27	50	63
16	domain16	33	54	62	32	59	21	35	25	27	31	54	63	26	39	22	29	48	63	21	60	40	29	51	47
17	domain17	24	50	77	35	47	27	36	41	29	20	45	83	20	32	21	33	56	41	17	48	51	24	47	55
18	domain18	38	37	73	30	38	50	25	17	26	42	44	47	17	37	16	30	53	70	27	45	34	26	49	60
19	domain19	4	6	10	2	8	8	0	6	3	4	4	1	4	4	6	6	14	4	2	6	2	1	10	2
20	domain20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	domain21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	domain22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	domain23	0	0	0	0	4	0	0	0	0	0	10	16	0	0	0	0	22	0	0	0	0	0	0	4
24	domain24	37	69	32	27	52	43	0	10	82	38	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	domain25	0	0	0	0	0	0	0	0	0	27	49	50	12	29	14	1	41	30	13	49	70	6	14	0
26	domain26	11	0	0	80	0	6	0	6	47	6	0	22	36	17	30	20	42	4	0	0	16	0	20	36
27	domain27	13	0	0	0	0	0	0	0	0	0	0	0	0	27	62	73	186	48	0	0	23	69	121	178
28	domain28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	domain29	14	36	42	28	16	31	21	24	31	14	48	31	15	23	10	22	28	55	17	52	29	16	26	22
30	domain30	0	16	33	0	15	9	1	3	0	5	17	37	0	16	2	8	18	45	4	12	11	2	30	19
31	domain31	21	36	36	14	51	46	17	23	23	10	26	42	13	28	22	24	32	37	21	33	14	11	28	23
32	domain32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	domain33	2	0	2	3	19	8	2	0	0	2	17	17	0	5	0	8	29	24	0	35	9	0	40	36
34	domain34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	domain35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	domain36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
37	domain37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	domain38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	domain39	1	5	6	7	4	8	3	1	2	1	4	8	5	8	2	6	3	6	2	4	4	0	0	3
40	domain40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
41	domain41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

5.3 IP アドレス別での検知数

次に，検知数が上位 1 の IP アドレス「domain1」及び上位 2 の「domain2」について，時間別，port 別での分析を行った．

（１）「domain1」

攻撃先 port を基準として比較を行ったところ，表 4 のとおり NICTER 及び NORSE とも同一の時間帯，同一の port において検知されていることが判明した．

表４　「domain1」の port 別検知数

nicter

攻撃先ポート	サービス名／時間	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
8080	8080	###	###	258	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	###	###	###
21	ftp	0	0	###	###	963	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	560
53	dns	0	0	0	0	632	###	###	90	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	smtp	0	0	0	0	0	0	0	###	###	952	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	ssh	0	0	0	0	0	0	0	0	0	889	###	###	0	0	0	0	0	0	0	0	0	0	0	0
3389	rdp	0	0	0	0	0	0	0	0	0	0	0	287	###	###	384	0	0	0	0	0	0	0	0	0
23	telnet	0	0	0	0	0	0	0	0	0	0	0	0	0	0	###	###	949	0	0	0	0	0	0	0
80	http	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	750	###	###	0	0	0	0	0
443	https	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	147	###	###	525	0	0

norse

攻撃先ポート	サービス名／時間	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
8080	8080	111	220	199	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	233	202
21	ftp	0	0	51	135	200	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
53	dns	0	0	0	0	0	135	107	39	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	smtp	0	0	0	0	0	0	0	66	119	78	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	ssh	0	0	0	0	0	0	0	0	0	18	192	280	26	0	0	0	0	0	0	0	0	0	0	0
3389	rdp	0	0	0	0	0	0	0	0	0	0	0	0	97	130	61	0	0	0	0	0	0	0	0	0
23	telnet	0	0	0	0	0	0	0	0	0	0	0	0	0	0	48	118	193	8	0	0	0	0	0	0
80	http	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	263	118	23	0	0	0	0
443	https	21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	179	155	101	0	0

また，NORSE でどこの国で観測されているかを時間別に確認したところ，21 ヶ国で観測されていることが判明した．

表５　「domain1」の NORSE での検知数

nicter

国名	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
日本	1704	1578	1668	1723	1595	1621	1753	1580	1653	1841	1763	1730	1744	1680	1821	1702	1699	1780	1711	1677	1747	1752	1750	1677

norse

国名	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
アメリカ	54	185	202	65	136	87	48	48	58	35	159	211	52	77	52	46	138	224	52	156	112	56	188	162
ドイツ	6	2	4	2	4	6	2	1	0	7	3	3	3	1	5	6	2	4	4	1	4	3	4	1
ベルギー	3	2	0	2	2	0	0	1	0	2	4	0	4	0	0	2	2	4	0	0	2	2	2	0
タイ	3	2	6	4	3	4	4	6	6	0	2	4	5	2	2	10	0	2	5	5	3	2	3	4
オーストリア	2	1	4	2	5	3	6	5	2	0	0	7	4	8	0	8	2	2	6	6	2	5	4	2
フランス	9	3	0	4	6	6	4	4	6	0	4	2	10	2	1	2	6	1	6	5	4	2	4	4
ポーランド	6	2	3	5	4	4	4	4	2	5	4	6	0	2	10	4	4	4	4	4	3	0	2	2
カナダ	2	2	2	4	0	0	2	2	0	4	0	2	2	2	3	2	0	2	0	4	0	2	0	2
リヒテンシュタイン	4	0	4	0	4	2	4	2	4	0	0	4	0	2	4	0	3	2	4	2	2	1	2	0
スペイン	8	4	2	3	8	8	4	3	10	7	5	6	8	4	6	8	4	2	10	2	4	8	6	2
ポルトガル	10	2	3	2	10	6	1	6	8	5	0	9	8	3	6	6	3	4	7	7	2	10	0	8
ノルウェー	4	2	2	7	0	1	2	3	4	2	0	8	2	8	0	6	4	6	4	0	5	4	0	3
オーストラリア	8	0	2	10	0	0	6	4	4	5	2	0	0	0	0	0	0	0	0	0	0	0	0	0
ブルガリア	2	0	0	2	0	2	0	0	0	3	0	0	1	0	0	2	0	0	0	2	0	0	0	0
アイスランド	4	6	2	2	5	2	7	2	4	3	0	4	6	3	4	2	8	0	9	1	4	4	2	7
イギリス	4	2	4	9	0	3	3	2	6	2	2	5	8	2	4	2	6	6	2	2	4	6	6	2
香港	3	3	4	7	2	6	1	5	3	4	1	6	4	5	2	2	6	2	2	4	2	4	5	2
イタリア	0	2	0	2	0	0	2	0	0	2	0	0	1	0	2	0	2	0	1	1	2	1	0	0
ルーマニア	0	0	6	1	2	2	2	3	0	2	2	3	0	2	4	2	1	2	2	0	0	3	0	1
シンガポール	0	0	0	2	7	3	5	4	2	6	4	0	5	5	4	6	2	0	0	0	0	0	0	0
トルコ	0	0	0	0	2	2	0	0	0	2	0	0	0	2	0	2	0	4	0	0	0	2	5	0

（２）「domain2」

上記（１）と同様に攻撃先 port を基準として比較を行ったところ，時間帯での検知に差異があることが判明した．

表６　「domain2」の port 別検知数

nicter

攻撃先port	サービス名／時間	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
8080	プロキシ	0	0	0	0	###	0	###	0	###	0	###	0	###	0	###	0	###	###	0	###	0	0	0	0
3128	プロキシ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	###	0	###	0

norse

攻撃先port	サービス名／時間	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
8080	プロキシ	39	365	23	99	40	291	44	66	79	50	122	38	96	35	87	57	84	127	97	113	8	0	0	0
3128	プロキシ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	70	57	172	44

また，国別で比較したところ，日本とは異なる時間帯で検知していることが判明した．

表７　「domain2」の NORSE での検知数

nicter

攻撃先／時間	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
日本	0	0	0	0	###	0	###	0	###	0	###	0	###	0	###	0	###	###	0	###	###	0	###	0

norse

攻撃先／時間	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
トルコ	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ドイツ	4	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
アメリカ	6	345	5	80	2	255	8	43	46	10	87	8	60	8	63	18	58	95	68	76	35	40	134	10
ポルトガル	16	0	8	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
オーストラリア	10	0	8	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ベルギー	2	2	2	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
スペイン	0	16	0	5	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
イタリア	0	2	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
リヒテンシュタイン	0	0	0	6	0	0	0	2	0	4	0	2	0	3	0	4	0	0	6	0	0	4	0	2
ポーランド	0	0	0	8	0	0	0	4	0	10	0	8	10	0	6	0	0	0	10	0	0	8	0	4
オーストリア	0	0	0	0	1	0	10	0	8	0	10	0	6	0	6	8	4	6	0	6	8	0	8	0
香港	0	0	0	0	8	0	10	0	3	0	3	8	0	3	0	4	6	10	0	8	10	0	0	8
フランス	0	0	0	0	5	0	8	0	8	0	6	8	0	3	0	3	8	6	0	10	3	0	0	8
ノルウェー	0	0	0	0	4	0	0	0	0	10	0	0	0	8	0	8	0	0	0	4	0	0	0	2
アイスランド	0	0	0	0	6	0	0	7	0	6	0	4	8	0	6	0	0	0	2	0	8	0	8	0
タイ	0	0	0	0	4	0	0	10	0	10	0	0	0	10	0	7	0	0	6	0	0	5	0	10
イギリス	0	0	0	0	8	0	0	0	10	0	10	0	8	0	0	3	4	6	0	6	10	0	10	0
ブルガリア	0	0	0	0	0	0	4	0	2	0	2	0	2	0	2	2	2	0	1	2	0	0	2	0
カナダ	0	0	0	0	0	0	4	0	2	0	4	0	2	0	4	0	2	4	4	1	0	0	4	0
シンガポール	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	6	0

以上のこのことから NICTER 及び NORSE で観測されるダークネットトラフィックには相関関係があることが判明し，日本及び世界で観測されるダークネット網のトラフィックデータを分析することで，日本と世界に対して同じようにスキャン等の活動を行っていることや，日本だけではなく世界に対してスキャン等の活動を行っていることなどがわかった．

次に，世界規模でのニュースとなった事件につき，ダークネット網と相関関係がないかどうかみていく．

5.4 世界規模でのニュースとなった事件との相関分析

世界規模でニュースとなった事件として，香港で起こった反政府デモがある．このデモは 2014 年 9 月 27 日から行ったものであり，このデモとダークネットトラフィックに相関関係があるかどうか NORSE のデータで比較を行ったところ，香港宛のパケットで特定の IP アドレス及び port の検知数が非常に多いことが判明した．

図 7 の香港宛攻撃元 IP アドレスで確認すると，香港から香港宛のパケットを非常に多く検知していることがわかる．

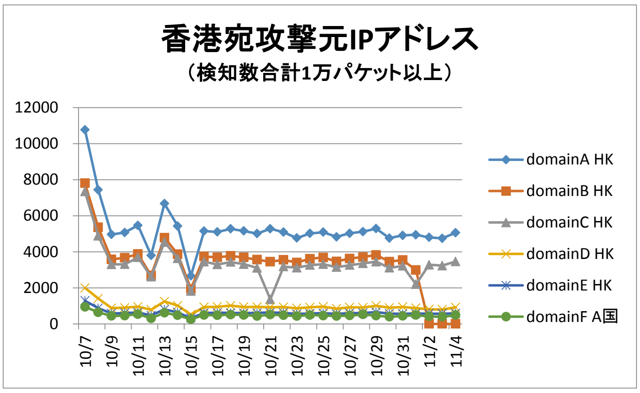


図 7　香港宛攻撃元 IP アドレス検知数

また，図 8 の香港宛攻撃 port 番号で確認すると，特定のポート「1947」,「138」,「17500」の 3 つが非常に多いことがわかる．

さらに，ポート「1947」,「138」,「17500」の攻撃元 IP アドレスを調べたところ，すべて香港の IP アドレスであることが判明した．

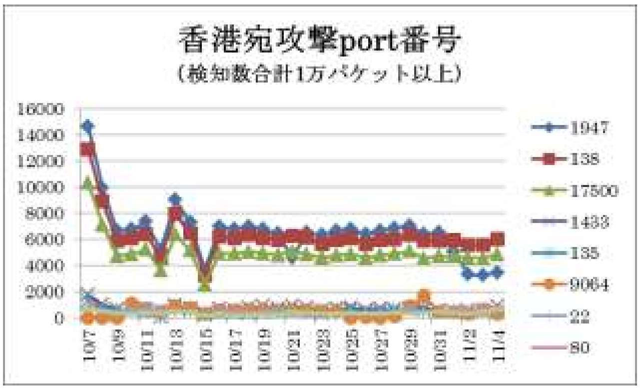


図８　香港宛攻撃 port 番号検知数

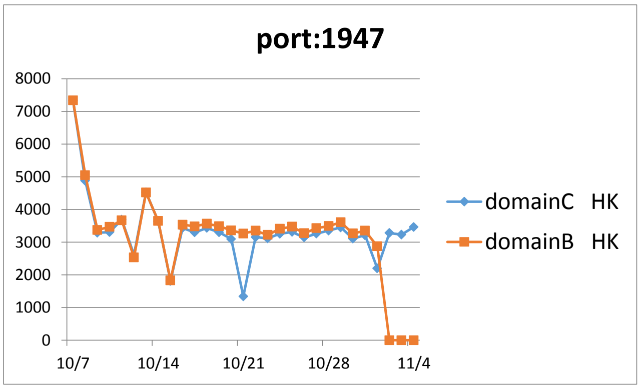


図９　port:1947 の IP アドレス検知数

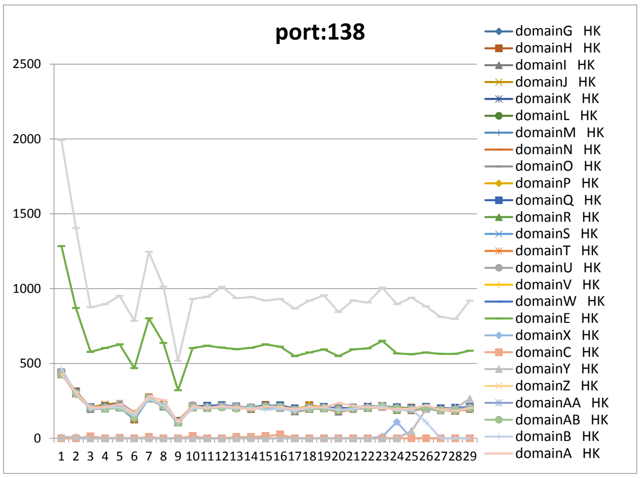


図１０　port:138 の IP アドレス別検知数

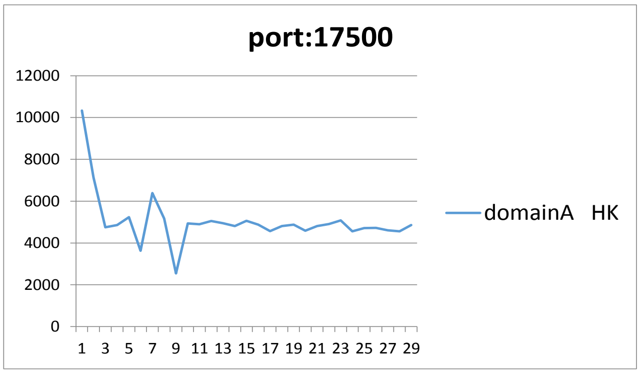


図１１　port:17500 の IP アドレス別検知数

次に，攻撃元 IP アドレスで観測された香港の IP アドレス群を香港以外の国でも検知していないか調べたところ，表８のとおりすべて香港のみで検知していることが判明した．なお，NICTER においては，検知がなかった．

表８　香港宛 IP アドレスの全体及び香港宛の検知数

項目	IPアドレス	国	10/7	10/8	10/9	10/10	10/11	10/12	10/13	10/14	10/15	10/16
検知数全体	domainA	HK	10765	7434	4960	5067	5462	3798	6669	5425	2660	5150
香港宛の検知数			10765	7434	4960	5067	5462	3798	6669	5425	2660	5150
検知数全体	domainB		7804	5352	3569	3672	3874	2684	4782	3864	1937	3734
香港宛の検知数			7804	5352	3569	3672	3874	2684	4782	3864	1937	3734
検知数全体	domainC		7338	4880	3302	3305	3690	2612	4536	3633	1813	3450
香港宛の検知数			7338	4880	3302	3305	3690	2612	4536	3633	1813	3450
検知数全体	domainD		1993	1404	875	896	951	784	1245	1012	518	931
香港宛の検知数			1993	1404	875	896	951	784	1245	1012	518	931
検知数全体	domainE		1284	870	577	603	627	468	801	636	321	603
香港宛の検知数			1284	870	577	603	627	468	801	636	321	603

項目	IPアドレス	国	10/17	10/18	10/19	10/20	10/21	10/22	10/23	10/24	10/25	10/26
検知数全体	domainA	HK	5100	5269	5153	5005	5276	5086	4763	5015	5083	4828
香港宛の検知数			5100	5269	5153	5005	5276	5086	4763	5015	5083	4828
検知数全体	domainB		3691	3770	3688	3562	3453	3546	3403	3614	3679	3460
香港宛の検知数			3691	3770	3688	3562	3453	3546	3403	3614	3679	3460
検知数全体	domainC		3297	3433	3309	3104	1357	3177	3114	3258	3312	3143
香港宛の検知数			3297	3433	3309	3104	1357	3177	3114	3258	3312	3143
検知数全体	domainD		945	1011	936	944	920	931	866	919	955	843
香港宛の検知数			945	1011	936	944	920	931	866	919	955	843
検知数全体	domainE		618	606	595	604	627	612	549	573	594	549
香港宛の検知数			618	606	595	604	627	612	549	573	594	549

項目	IPアドレス	国	10/27	10/28	10/29	10/30	10/31	11/1	11/2	11/3	11/4
検知数全体	domainA	HK	5023	5117	5283	4755	4908	4943	4795	4747	5059
香港宛の検知数			5023	5117	5283	4755	4908	4943	4795	4747	5059
検知数全体	domainB		3624	3703	3821	3450	3543	2980	0	0	0
香港宛の検知数			3624	3703	3821	3450	3543	2980	0	0	0
検知数全体	domainC		3260	3352	3451	3107	3211	2195	3279	3231	3463
香港宛の検知数			3260	3352	3451	3107	3211	2195	3279	3231	3463
検知数全体	domainD		921	907	1006	896	939	881	811	797	920
香港宛の検知数			921	907	1006	896	939	881	811	797	920
検知数全体	domainE		594	600	651	567	561	573	564	564	585
香港宛の検知数			594	600	651	567	561	573	564	564	585

このことから，香港に対して何らかの活動が行われていた可能性がある．ここで取り上げた三つのポートは主に以下の用途で利用するものである．

（１）port:1947

Port:1947 の主な用途して，HASP License Manager との利用がある．ソフトウェアのライセンスマネジャーとして利用することが可能であり，ソフトウェアの仕様として Port:1947 を利用して，ネットワーク越しにアクセス管理やログを取得可能な製品もある．

（２）port:138

Port:138 は，ファイル共有として利用することが可能なポートであり，家庭内などの閉じたネットワークでの利用が原則であり，外部に対して開放している場合，外部からの侵入口となってしまう危険性がある．通常は，ポートを閉じておくことが常識となっている．

（３）port:17500

Port:17500 は，Dropbox で利用する LAN 同期を必要とする場合に必要となるポートである[12]．LAN 同期を有効とした場合，同一ネットワークにブロードキャストアドレスを大量に送信することが確認されている．実機を用いて検証したところ，図１１のとおりブロードキャストアドレスが大量に送信されることが確認された．

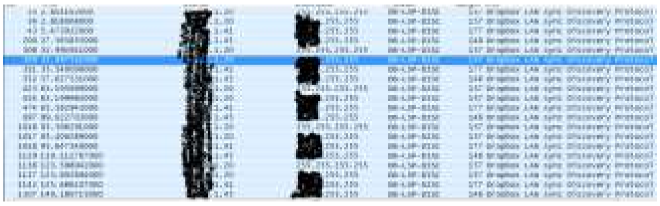


図１１　Dropbox 利用時のブロードキャスト

香港のデモでは，iCound に大規模なハッキング攻撃があった事件が報道[13]され，その目的として，香港で続く大規模デモの写真や動画が中国本土で拡散するのを防ごうとした狙いがあったのではないと推測されている．また，当局によるインターネット規制が多くあったことから，SNS 等のソーシャルメディアの利用が加速され，その一環として，ファイルを共有できる Dropbox の利用が促進された可能性がある．これにより，port:17500 が大量に観測されたのではないだろうか.

また，推測の域は出ないが，port:1947,138 は香港に対して何らかのスキャン等の活動が行われていた可能性がある.

なお，2015 年 1 月 19 日から 27 日までの期間で，NORSE で同様の IP アドレスから香港宛への観測状況を確認したところ，１件も確認されなかった．このことから，特定期間で利用された IP アドレス群であった可能性がある.

6.　まとめと今後の課題

本稿では，NICTER 及び NORSE で観測されるダークネットトラフィックの相関分析を行った．分析の結果，日本と世界で観測されるダークネットトラフィックには相関関係があることがわかった．また，どちらか一方だけでは不明なことでも双方で分析を行うことで，新たな特徴を発見することができることもわかった．さらに，世界規模でのニュースとの分析においても，ダークネットトラフィックを分析することにより，ターゲットとされているポートや地域を推測することが可能であることがわかった.

今後は，より広範囲の期間を対象として分析を行うことで，日本と世界で観測されるダークネットトラフィックの傾向を見出すことができると考えられる.

7.　謝辞

本研究では，NICTER が保有しているサイバーセキュリティ情報を遠隔から安全に利用するための分析基盤（NONSTOP）にて提供されるダークネットデータを利用した. 貴重なデータセットを提供して頂いた NICTER の関係者各位に深く感謝します.

8.　参考文献

1)　トレンドマイクロ株式会社,”2013 年国内における持続的標的型攻撃の分析” https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81 (最終閲覧日　2015/01/22)
2) 独立行政法人　情報通信研究機構, http://www.nict.go.jp/　(最終閲覧日　2015/01/22)
3) 独立行政法人　情報通信研究機構,”インシデント分析センター NICTER の研究開発概要”，情報通信研究機構季報 Vol.57 Nos.3/4 2-1
4) 独立行政法人　情報通信研究機構,”第 2 部 ダークネットからライブネットへーサイバーセキュリティ研究最前線ー”, NICT 情報通信セキュリティシンポジウム 2014〜情報セキュリティ技術の現状と今後〜
5) NORSE Corporation, http://www.NORSE-corp.com/darklist.html(最終閲覧日　2015/01/22)
6) NORSE IPViking Live, http://map.ipviking.com/(最終閲覧日 2015/01/22)
7) 総務省,”政府における情報セキュリティ政策の取組について”,2014.1.15
8) CAIDA, http://caida.org/home/(最終閲覧日　2015/01/22)
9) M.Bailey,E.Cooke,F.Jahanian,A.Myrick, and S.Sinha,”Practical darknet measurement.”Information Sciences and Systems,2006 40th Annual Conference on,pp.1496-1501,IEEE,2006.
10)　‘SPAMHAUS’http://www.spamhaus.org/(最終閲覧日 2015/01/22)
11)　鈴木将吾，小出駿，牧田大祐，吉岡克成，　松本勉，笠間貴弘，衛藤将史，井上大介，村上洸介，島村隼平“複数国ダークネット観測による攻撃の局地性分析”CSS2014
12)　LAN 同期について, https://www.dropbox.com/ja/help/137(最終閲覧日：2015/2/8)
13)　中国関与？　ｉＣｌｏｕｄに大規模ハッキング攻撃　香港デモ写真削除狙う, http://www.sankei.com/world/news/141023/wor1410230016-n1.html(最終閲覧日：2015/2/8)