Vol.2015-CSEC-69 No.17
Vol.2015-IOT-29 No.17
2015/5/21

ハニーポットによる大分大学における ダークネット宛通信の分析

池部 実[1,a)]　宮崎 桐果[1]　吉田 和幸[2]

概要：大分大学が保有する IP アドレスのうち，未使用である/24 のセグメントに，ハニーポットを設置し，2014 年 7 月から 2015 年 2 月までの 8 ヶ月間通信を観測した．未使用の IP アドレスをダークネットと呼ばれている．ダークネット宛の通信は，攻撃者の不正な活動に起因することが多い．そこで，ダークネットを観測することで大分大学宛の不正通信の傾向を分析する．ハニーポットが受信した通信を，ポート番号や送信元 IP アドレスなどの傾向を分析した．また，TCP/80 番ポートに対する通信は，ハニーポットにおいて，擬似的に応答するように設定した．TCP/80 番ポートに送信された HTTP メソッドや要求 URL を分析した．また，学内で稼働している Web サーバのログとハニーポットのログを照合した．これらの大分大学のダークネットで観測した不正通信の分析結果について報告する．

キーワード：ネットワークセキュリティ，ダークネット，ハニーポット，HTTP

Analysis of Darknet traffic on Oita University by Honeypot

Ikebe Minoru[1,a)]　Miyazaki Touka[1]　Yoshida Kazuyuki[2]

Abstract: We have set up a honeypot on an unused IP address space of Oita University. A unused IP address space of network called darknet. The cause of packets to the darknet is malicious activities of attackers. We have observed the darknet traffic by using the honeypot from July 2014 to February 2015. Therefore, we analyze malicous activities to the Oita University. We analyzed port numbers and source IP addresses. Also, our honeypot system replies a HTTP response message to a HTTP request message from attackers. We analyzed HTTP method and URL from the attackers. And, we compared the honeypot's logs and web server's logs. In this paper, we report the analysis of the darknet traffic to the Oita University.

Keywords: Network Security, Darknet, Honeypot, HTTP

1. はじめに

インターネットの普及に伴い，ネットワークを通じて様々な情報がやりとりされるようになってきた．Web ページの閲覧や電子メールを始めとしたコミュニケーションに留まらず，行政手続きや電子決済などのサービスもインターネットを介して提供されている．そのため，インターネットは社会的基盤のひとつとして我々の生活に不可欠な存在となってきている．一方で，インターネットを利用することによって様々な脅威にさらされる危険性がある．2014 年においては，2013 年に引き続きサイバー攻撃・犯罪の金銭被害が拡大している [1]．そのため，大学・研究機関などの組織においても，セキュリティを強化していくことが重要となってきている．

ネットワーク管理者が様々な脅威を発見するための手段のひとつとして，ダークネット観測がある．ダークネットは，インターネット上で到達可能な IP アドレスのうち，組

[1] 大分大学工学部知能情報システム工学科
Department of Computer Science and Intelligent Systems, Faculty of Engineering, Oita University
[2] 大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita University
[a)] minoru@oita-u.ac.jp

表 1 Honeyd で観測したプロトコル別コネクション数

プロトコル	コネクション数 (件)
TCP	8,296,844
UDP	2,729,997
ICMP	1,422,820
SCTP	701
その他 (gre(47), unknown(17))	2
合計	12,450,364

織内で未割り当てな IP アドレス空間である．ダークネットは未使用の IP アドレスであるため，通常はダークネットに対してパケットが送信されることはほとんどない．しかしながら，実際にはダークネット宛へのパケットが大量に観測されているのが現状である．ダークネット宛のパケットの多くは，以下のような不正な活動に起因するものと報告されている [2].

- リモートエクスプロイト型マルウェアが次の感染対象を探査するためのスキャン
- マルウェアが感染対象の脆弱性を攻撃するためのエクスプロイトコード
- 送信元 IP アドレスが詐称された DDoS 攻撃を被っているサーバからの応答であるバックスキャッタ

そこで，我々は大分大学宛の不正通信を分析するため，クラス C 相当のダークネットにハニーポットを設置して，通信状況を分析している [3]．TCP/80 番ポートに対しては，送信されたパケットに対して HTTP レスポンスを応答するように設定した．その他のポートに対しては，応答していない．

本論文では，ハニーポットを 2014 年 7 月 15 日から 2015 年 2 月 25 日までの約 8 ヶ月間稼働させ，その通信状況を分析した結果を報告する．また，HTTP リクエストに対して，HTTP レスポンスを応答するように設定していた TCP/80 に対する分析結果を述べる．本論文で分析した期間に，Shellshock を狙った Web サーバに対する攻撃を多数観測した．ハニーポット上の Web サーバに対する攻撃を分析した結果を報告する．

2. ハニーポットのログ解析

ハニーポットには，オープンソースソフトウェアの Honeyd を用いた．クラス C 相当のネットワークサイズのダークネットに Honeyd を設置した．Honeyd に対して，第 4 オクテットを 3 から 253 までの 251 個の IP アドレスを割り当て，ダークネットに対する通信を観測した．

本論文で対象としたハニーポットのログ収集期間は，2014 年 7 月 15 日 12 時 10 分 59 秒から 2015 年 2 月 25 日 13 時 18 分 15 秒である．この期間，一部，ログを収集できていない期間が存在する．観測期間中，Honeyd で観測したコネクション総数は，12,450,364 件であった．プロトコル別のコネクション数を表 1 に示す．

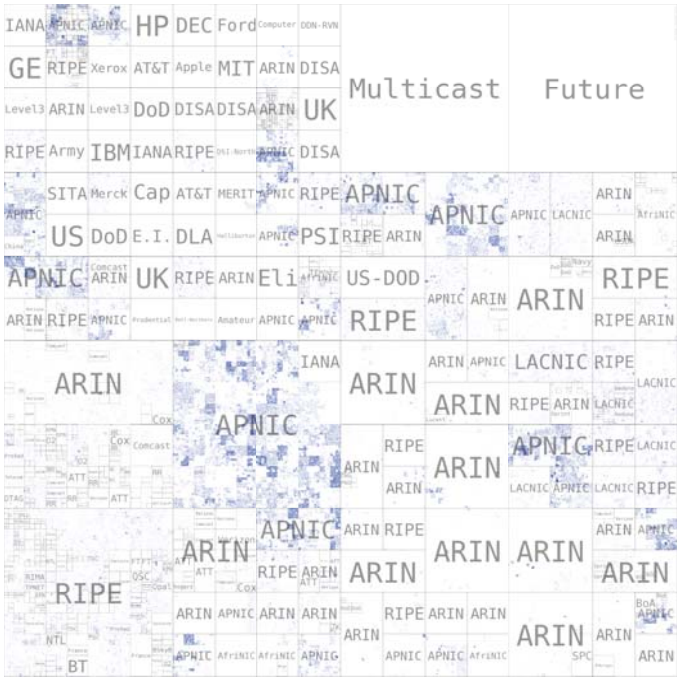

図 1 送信元 IP アドレスの可視化 (ヒルベルト空間曲線)

表 2 送信元 IP アドレス数 (上位 10 ヶ国)

CC	送信元 IP アドレス数
CN	328,537
KR	43,346
TW	31,725
JP	25,715
US	18,971
HK	10,422
TH	9,692
RU	9,317
BR	5,750
ID	4,707

Honeyd で観測したコネクションの送信元 IP アドレス数は，562,062 個であった．すべての送信元 IP アドレスをヒルベルト空間曲線にて可視化した (図 1)．また，送信元 IP アドレスを GeoIP にて国別コードを調べた結果 [*1] の上位 10 件を表 2 に示す．APNIC に割り当てられた IP アドレスから非常にアクセスが多いことが分かる．

また，プロトコル別のアクセスが多い宛先ポート番号，ICMP のタイプを表 3 から表 5 に示す．

TCP の宛先ポート番号の上位 10 種類を表 3 に示す．TCP の宛先ポート番号は，HTTP(80/TCP) が一番多い結果であった．今回設置した Honeyd の設定では，通常のポートは，TCP 3way handshake の SYN パケットに対して，応答しない．しかし，80 番ポートは TCP 3way handshake を確立し，送信された HTTP リクエストに対してプログラムにより擬似的に HTTP レスポンスを返すように設定しているため，2 番目の SSH よりも 3 倍近いコネクション

[*1] 2015 年 3 月 30 日の時点の最新データを用いた

表 3 TCP 宛先ポート番号 (上位 10 種類)

宛先ポート番号	コネクション数
80	1,853,361
22	613,612
8080	605,441
443	430,820
3389	409,198
3128	326,215
21320	200,057
1080	196,216
25	153,952
21	128,443

表 4 UDP 宛先ポート番号 (上位 10 種類)

宛先ポート番号	コネクション数
53	350,955
123	244,936
1900	194,409
161	120,790
19	93,964
53413	83,308
623	64,829
17	48,833
5060	48,702
3076	35,083

表 5 ICMP タイプ (上位 5 種類))

ICMP タイプ (コマンド)	コネクション数
8(0)	100,4378
3(10)	196,141
3(3)	93,703
0(0)	89,310
11(0)	15,918

数となっていると考えられる．上位の残りは，リモートアクセスサービスや Web プロキシの探索が多くなっている．

UDP の宛先ポート番号の上位 10 種類を表 4 に示す．上位には，応答の増幅率が大きい DNS(53/UDP)，NTP(123/UDP)，SNMP(161/UDP) が多い結果であった．ほかにも，SSDP で使われる 1900 番ポートへのコネクションが多かった．

ハニーポットに送信された ICMP のタイプとコマンドの上位 5 件を表 5 に示す．ICMP パケットのうち，ICMP Echo Request が多くを占めていた．ICMP パケットの送信元 IP アドレスを調査すると，ICMP Echo Request メッセージを送信しているインターネット計測プロジェクトに関連するホスト名が多くを占めていた．

Honeyd のログ解析プログラム (honeydsum.pl) を用いて分析した結果を以下に示す．251 個の IP アドレスに対するアクセス数を分析した．Honeypot として設定している IP アドレス別に，送信元 IP アドレス数，宛先ポート数 (TCP/UDP 区別なし)，コネクション数を調査した．表 6 に，251 個の IP アドレスに対する送信元 IP アドレス数，宛先ポート数，コネクション数の平均値，最小値，最大値を示す．

表 6 IP アドレスあたりの平均値

	送信元 IP アドレス数	宛先ポート数	コネクション数
平均値	9,870.69	1,300.92	46,060.68
最小値	15,1742.00	1,045.00	34,323.00
最大値	7,018.00	7,149.00	272,018.00

表 7 宛先 IP アドレス上位 8 件

宛先 IP アドレス	送信元数	宛先ポート数	コネクション数
133.37.X.58	15,1742	7,149	272,018
133.37.X.27	33,265	3,380	84,804
133.37.X.121	29,383	2,573	81,919
133.37.X.110	26,283	2,506	78,810
133.37.X.116	32,048	3,014	77,654
133.37.X.101	22,853	3,173	77,164
133.37.X.183	26,572	1,948	66,284
133.37.X.175	14,004	1,489	44,183

表 8 133.37.X.58 におけるプロトコル別コネクション数

	133.37.X.58	251 個の平均
TCP	32,042	33,055.16
UDP	236,422	10,876.48
ICMP	3,554	5,668.61
合計	272,018	49,600.24

表 9 133.37.X.58 に対する送信元 IP アドレス数

	送信元 IP アドレス数	コネクション数	CC
1	218.77.A.B	2,328	CN
2	218.77.A.C	719	CN
3	61.240.D.E	645	CN
4	218.77.F.G	627	CN
5	93.174.H.I	603	NL
6	124.232.J.K	513	CN
7	61.240.L.M	505	CN
8	61.240.L.N	490	CN
9	93.180.O.P	476	RU
10	61.160.Q.R	469	CN

ハニーポットとして利用している 251 個の IP アドレスのうち，8 個の IP アドレスに対して，他の IP アドレスよりも多くの送信元からのアクセスを観測した (表 7)．

ハニーポットとして利用している IP アドレスに対するアクセスの送信元 IP アドレス数は平均 1 万弱であったのに対し，上記の 8 つの IP アドレスに対しては，平均より多くの送信元 IP アドレスからコネクション数であった．とくに，133.37.X.58 については，平均より 15 倍の 15 万の送信元 IP アドレスからアクセスがあった．

133.37.X.58 に対するコネクションの分析結果を示す (表 8)．表 8 に示すように，UDP コネクションが大量に観測されていた．

他の 250 個の IP アドレスの傾向を分析すると，22/TCP，

表 10　133.37.X.58 に対する宛先ポートのコネクション数

	宛先ポート番号	コネクション数
1	29700/UDP	5,951
2	42808/UDP	3,832
3	80/TCP	3,711
4	38954/UDP	3,475
5	59969/UDP	3,269
6	12369/UDP	3,013
7	22/TCP	3,006
8	17434/UDP	2,968
9	22572/UDP	2,820
10	32025/UDP	2,759

80/TCP，8080/TCP，3389/TCP，443/TCP，53/UDP などが多い．一方，この 133.37.X.58 に対しては 1024 番以降の登録済みポートやエフェメラルポートに対して多くの UDP コネクションが確認された．このコネクションは，SIP 等を狙ったアクセスであると考えられる．133.37.X.58 は他の 250 個の IP アドレスと同一の設定であり，このホストだけが集中的に SIP を狙われた理由は不明である．

251 個のハニーポットの IP アドレスのうち約 72%に対して，表 9 に示した 218.77.A.B からのコネクションが一番多い結果であった．この送信元 IP アドレスはどの IP アドレスに対しても，2,300 前後のコネクションを送信していた．

宛先ポート番号のうち，コネクション数が多かった 9 つのポート (22/TCP，80/TCP，443/TCP，3389/TCP，8080/TCP，53/UDP，123/UDP，161/UDP，1900/UDP) を IP アドレス別にコネクション数をグラフ化した (図 2)．SSH(22/TCP) は，IP アドレスの若い番号に対して，多くのコネクションを観測した．他の 8080/TCP，3389/TCP，1900/UDP においても同様の傾向が観測された．一方，443/TCP，53/UDP，123/UDP，161/UDP はどの IP アドレスに対してもほぼ一定のコネクション数を観測した．

観測した 8 ヶ月分の調査期間において，TCP/UDP/ICMP の 1 時間ごとのコネクション数をグラフ化した (図 3)．1 時間ごとのコネクション数で，ピークを観測したのは 2014 年 11 月 5 日 15:00 から 16:00，2014 年 11 月 10 日 0:00 から 1:00 であり，いずれも 80/TCP であった．これらの時間帯には，特定の IP アドレスからハニーポット全体に対して，大量の HTTP リクエストが送信されていた．

3. TCP/80 番ポートに対する応答結果分析

今回設置したハニーポットでは，TCP/80 のコネクションに対して，Perl プログラムにより擬似的に HTTP レスポンスを応答するように設定していた．

3.1 ハニーポットによるリクエスト収集

ハニーポットによる TCP/80 に対するコネクションの収集方法を以下に示す．TCP 3way handshake 確立後の挙動を示す (図 4)．以下の挙動は Perl プログラムによって実行している．

(1) 送信者が 133.37.X.4 宛に HTTP リクエストを送信
(2) Honeyd(133.37.X.2) は，133.37.X.4 宛の HTTP リクエストを収集
(3) Honeyd は送信者に対して，送信元を 133.37.X.4 として HTTP レスポンスを応答

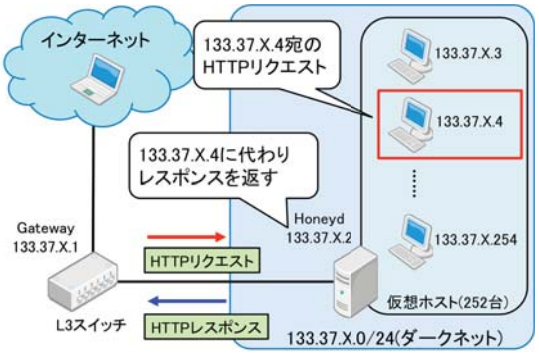

図 4　Honeyd による TCP 3way handshake 確立後の挙動

送信者からの HTTP リクエストの内容 (主に要求したファイル拡張子) に応じてステータスコード 200，404，500 を返すように設定していた．送信者から送られる HTTP リクエストを Honeyd が記録するログとは別に保存する．以下の内容をアクセスログとして，ファイルへ出力する．

(1) HTTP リクエスト受信時刻
(2) 送信元 IP アドレス
(3) 送信元ポート番号
(4) 宛先 IP アドレス
(5) 宛先ポート番号
(6) 送信元 OS(判明した場合のみ)
(7) HTTP リクエスト
(8) HTTP ヘッダ

3.2 HTTP リクエスト分析結果

ハニーポットで収集した TCP/80 に対するコネクションを収集し，分析した．リクエスト収集期間は 2014 年 7 月 15 日から 2014 年 11 月 13 日である．期間中のコネクション総数は 178,625 件，送信元 IP アドレス数は 9,729 個であった．コネクションを HTTP リクエストのメソッド別に分類した結果を表 11 に示す．表 11 のうち，GET メソッドによるリクエストの内訳を表 12 に示す．表 12 に示した HTTP GET メソッドによるリクエストには，特定ファイルの要求，ルートディレクトリ (/) の要求，http://からはじまる要求が含まれていた．http://からはじまる要求は，

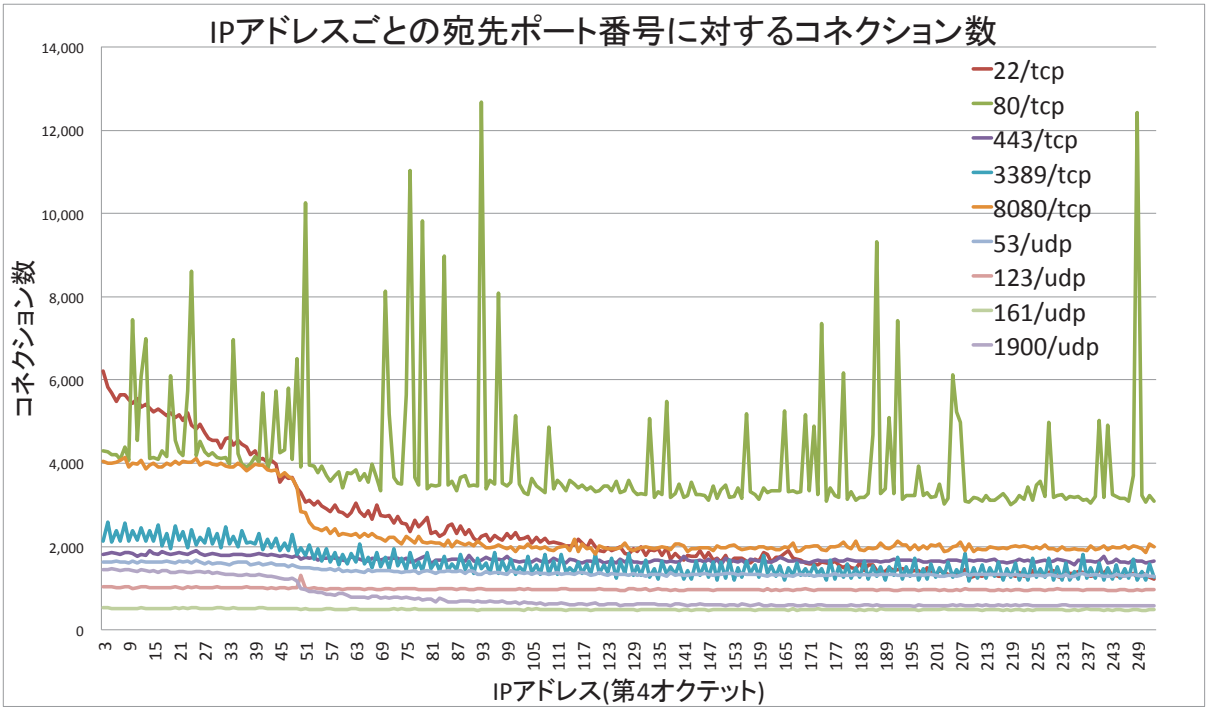

図 2 IP アドレスごとの宛先ポート番号コネクション数

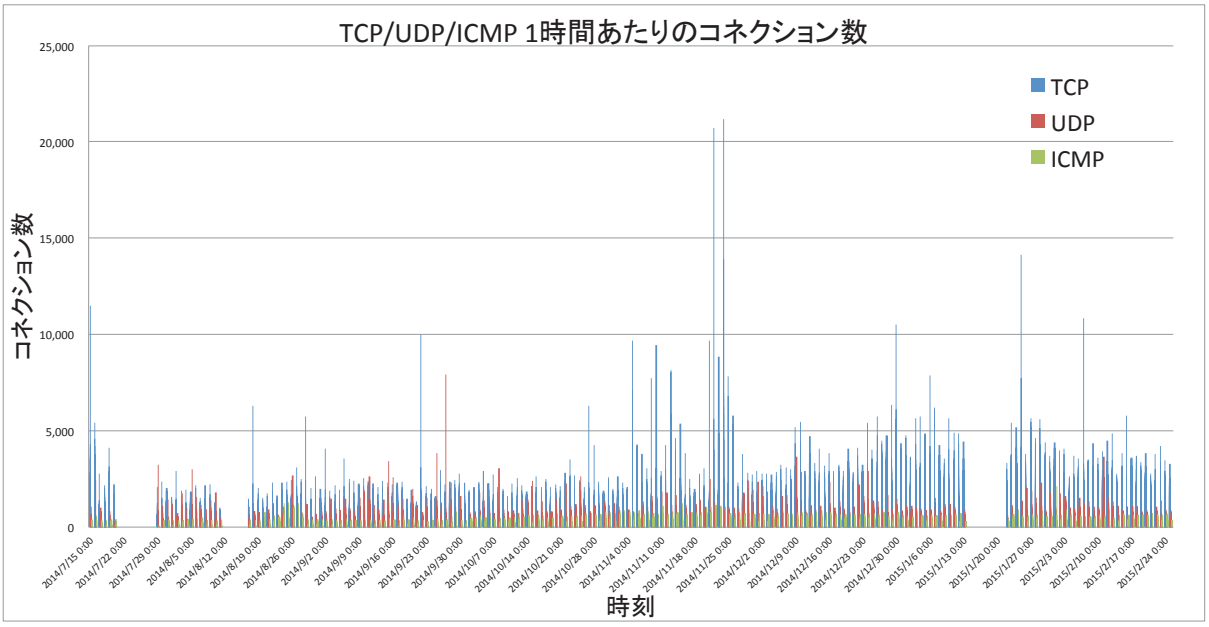

図 3 TCP/UDP/ICMP の 1 時間ごとのコネクション数

オープンプロキシの探索活動であると考えられる．佐藤らの報告 [4] によると，ハニーポットで収集した HTTP リクエストより，リクエスト行で GET メソッドを用い，任意の URL を要求する HTTP リクエストが，オープンプロキシを探索する攻撃だと考察している．攻撃者はオープンプロキシを探索する際に，標的 Web サーバに HTTP リクエストを送信し，Web サーバの反応でオープンプロキシかを判断する．佐藤らが考察する攻撃者の挙動を図 5 に示す．

(a) オープンプロキシでない Web サーバに HTTP リクエストを送信する例

表 11 Honeyd で観測した HTTP リクエストのメソッド別コネクション数

メソッド	コネクション数	割合 (%)
GET	87,878	49.2
CONNECT	56,692	31.7
空行	26,369	14.8
HEAD	6,928	3.9
OPTIONS	502	0.3
POST	256	0.1
合計	17,8625	100.0

表 12　Honeyd で観測した HTTP GET メソッドのリクエスト内容

リクエスト	コネクション数	割合 (%)
特定ファイルの要求	40,346	45.9
ルートディレクトリの要求	25,406	28.9
http://からはじまる要求	22,126	25.2
合計	87,878	100.0

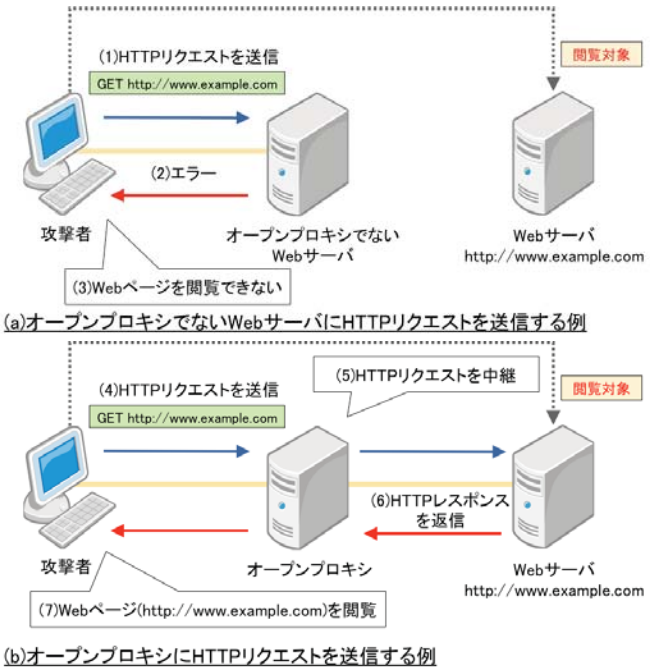

図 5　オープンプロキシの探索活動

(1) 攻撃者は閲覧対象 Web サーバの URL を含んだ HTTP リクエストを，標的 Web サーバに送信
(2) 標的 Web サーバは HTTP リクエストを中継しないため，攻撃者にエラーを返信
(3) 攻撃者は閲覧対象 Web サーバのページを閲覧できない

(b) オープンプロキシに HTTP リクエストを送信する例
(4) 攻撃者は閲覧対象 Web サーバの URL を含んだ HTTP リクエストを，標的 Web サーバに送信
(5) 標的 Web サーバはオープンプロキシであるため，閲覧対象 Web サーバに HTTP リクエストを中継
(6) 閲覧対象 Web サーバはオープンプロキシを経由して，攻撃者に HTTP レスポンスを返信
(7) 攻撃者は閲覧対象 Web サーバのページを閲覧できる

以上のように，攻撃者は閲覧対象 Web サーバのページを閲覧できるか否かで，宛先ホストがオープンプロキシかを判断していると佐藤らは考察している．

今回の調査期間において，特定のファイルを要求する HTTP リクエストに，Shellshock を狙った攻撃が存在した．Shellshock とは，UNIX 系 OS で用いられる bash(Bourne Again Shell) に発見された脆弱性である．HTTP ヘッダの User-Agent:以降に，“{ :;}; 任意のコマンド” を記述することで，脆弱性をもつサーバに対して任意のコマンドを実行することができる．Shellshock を狙った攻撃は，2014 年 9 月 25 日から 10 月 7 日までの期間に観測された．HTTP リクエストに，“() { :;};” が含まれていたリクエストは 1900 件観測した．今回観測したリクエスト例を図 6 に示す．

図 6 に示したように，送信者側が用意したホストに対して ping を実行するリクエストや，送信者側が用意したコンテンツを wget で取得してプログラムを実行させるリクエストを観測した．

3.3　ハニーポットと Web サーバのログ照合

前節まではダークネットへの通信の分析結果を述べた．ハニーポットにおいて，Shellshock を狙った HTTP リクエストを多く観測しており，メンテナンスされていない実際に稼働している Web サーバに対して Shellshock を狙った HTTP リクエストが送信された場合，乗っ取られる可能性がある．そこで，Web サーバのログを調べ，Shellshock の HTTP リクエスト状況を調べるとともに，ハニーポットと Web サーバのログを照合し，アクセスの傾向に違いがあるかを調査した．

本節では，ハニーポット宛の通信と実際に稼働している Web サーバ宛の通信を照合した結果について述べる．ダークネット宛の通信の送信元は，実際に Web サーバへどのようなアクセスをしているのかを調査するために，前節まで述べたハニーポット (253 個の IP アドレス) のログと，2 台の学内の Web サーバのログを照合した．

学内の Web サーバのうち，1 台はとある学科の情報公開用 Web サーバで Apache，WordPress の環境で動作している (以下，Web サーバ 1 と呼ぶ)．もう 1 台は，アドレスハーベスタによる spam の宛先メールアドレス収集の挙動を調査するために設置している Web サーバ [5] であり，Apache で動作している (以下，Web サーバ 2 と呼ぶ)．Web ページは，HTML と Perl による CGI で提供されている．この Web サーバは，外部からのリンクがほぼないため，正規のユーザによるアクセスはほとんどない．

本調査では，Shellshock を観測した期間を含む 2014 年 9 月 14 日から 2014 年 10 月 14 日までの 1 ヶ月間の各サーバのログを用いて照合した．それぞれのサーバのログにおいて，確認された HTTP メソッド別のコネクション数を表 13 に示す．

3.3.1　Web サーバ 1 の傾向

Web サーバ 1 は，工学部のとある学科の情報提供用であるため，GET リクエストが圧倒的に多く，すべてのリクエストのうち，89.43%はステータスコード 200 を返していた．POST メソッドや HEAD メソッドは日本以外からのリクエストであった．Web サーバ 1 に対する Shellshock の攻撃は，8 件観測した．

```
User-Agent: () { :;}; /bin/bash -c “echo testing9123123”; /bin/uname -a
Referer: () { :; }; /bin/ping -c 1 104.131.0.69
User-Agent: () { :;}; /bin/ping -c 1 198.101.206.138
User-Agent: shellshock-scan (http://blog.erratasec.com/2014/09/bash-shellshock-scan-of-internet.html) Host:() { :; }; ping -c 23 209.126.230.74 Referer: () { :; }; ping -c 11 209.126.230.74
User-Agent: masscan/1.0 (https://github.com/robertdavidgraham/masscan) Host: () { :; }; wget 37.187.225.119/action.txt > /var/www/; wget 37.187.225.119/action.txt > /var/www/html/ Referer: () { :; }; wget 37.187.225.119/action.txt > /var/www/; wget 37.187.225.119/action.txt > /var/www/html/
User-Agent: () { :;}; /bin/bash -c “wget -O /var/tmp/ec.z 74.201.85.69/ec.z;chmod +x /var/tmp/ec.z;/var/tmp/ec.z;rm -rf /var/tmp/ec.z*”
```

図 6 Shellshock を狙った攻撃の例

表 13 各サーバで観測した HTTP リクエストのメソッド別コネクション数

メソッド	Honeyd	Web サーバ 1	Web サーバ 2
GET	33,404	87,439	809
CONNECT	15,016	83	0
空行	5,332	0	0
HEAD	1,479	24	22
OPTIONS	198	10	0
POST	96	4	1
合計	55,525	87,560	832

3.3.2 Web サーバ 2 の傾向

Web サーバ 2 は，外部からのリンクはほとんどないため，正規のユーザによるアクセスはほとんど観測しない．そのため，HTTP リクエストの内容は，tmUnblock.cgi を要求するリクエスト，phpMyAdmin の脆弱性を探索するリクエストなどを観測した．Web サーバ 2 に対する Shellshock の攻撃は，10 件観測した．

3.3.3 3 つのサーバのログ照合結果

それぞれのサーバに対してアクセスしてきた送信元 IP アドレス数は，Honeyd は 2082 個，Web サーバ 1 は 2232 個，Web サーバ 2 が 183 個であった．これら 3 つのサーバで共通した送信元 IP アドレス数は，42 個であった．この 42 個の送信元 IP アドレスからのリクエストを図 7 に示す．ルートディレクトリを要求したリクエスト以外は，CGI や PHP などの脆弱性のあるスクリプトを探索するリクエストと考えられる．

Honeyd と Web サーバ 1 に共通した送信元 IP アドレスは 57 個，Honeyd と Web サーバ 2 に共通した送信元 IP アドレスは 58 個であった．

Web サーバ 1 と Web サーバ 2 へ送信されたリクエスト内容から攻撃者と判断した送信元 IP アドレスのうち，Honeyd サーバでは観測していない送信元 IP アドレスを観測した．Web サーバ 1 では 77 個，Web サーバ 2 では 124 個である．これらの送信元 IP アドレスからのリクエスト内容を調査したところ，Honeyd で観測したリクエスト内容と同様のリクエストを送信していた．今回の HTTP リクエストをボットネットにより，分散して送信していた可能性も考えられる．Honeyd や Web サーバに対する HTTP リクエストにもとづいた共通性の調査を今後実施する予定である．

```
GET /admin/config.php HTTP/1.0
GET /cgi-bin/test-cgi HTTP/1.0
GET /cgi-sys/defaultwebpage.cgi HTTP/1.0
GET /cgi-bin/count.cgi HTTP/1.1
GET /cgi-bin/php HTTP/1.0
GET /DefaultWS.asmx HTTP/1.1
GET /epgrec/do-record.sh HTTP/1.0 GET /epgrec/systemSetting.php HTTP/1.1 GET / HTTP/1.0
GET / HTTP/1.1
GET /etc/lib/pChart2/examples/index.php HTTP/1.1
GET /manager/html HTTP/1.1
GET /phpMyAdmin/scripts/setup.php HTTP/1.0
GET /web-console/ServerInfo.jsp HTTP/1.1
GET w00tw00t.at.ISC.SANS.DFind:) HTTP/1.1
HEAD /index.action HTTP/1.1
HEAD /login.do HTTP/1.1
HEAD /rom-0 HTTP/1.1
HEAD / HTTP/1.0
HEAD / HTTP/1.1
```

図 7 3 つのサーバに共通した送信元 IP アドレスからのリクエスト

4. おわりに

本調査では，大分大学のクラス C 相当のダークネットにハニーポットを設置し，そのアクセス傾向などを調査した結果を報告した．今後は，学内の Web サーバのログと Honeyd のログの照合を詳細にする他，我々が開発している不正通信検知システム [6] のログと Honeyd のログの照合を進めていく予定である．

また，本論文では，awk や sort，uniq など UNIX コマンドを組み合わせて，シェルスクリプトや Perl スクリプトなどで分析した．現在，様々なサーバログを統合管理するログ管理システムの研究・開発 [7] を進めており，そのシス

テム上で，Honeyd のログを収集してログを管理し，今回の分析で用いた UNIX コマンドを組み合わせて，集計したデータを容易に出力可能なスクリプトとデータ管理システムの開発を進める．

謝辞 本研究は，JSPS 科研費 25870558 の助成を受けたものです．

参考文献

[1] 情報処理推進機構 (IPA)：情報セキュリティ 10 大脅威 2015，（オンライン），入手先 ⟨http://www.ipa.go.jp/files/000044680.pdf⟩（参照 2015-3-26）．
[2] 井上大介：情報セキュリティ技術動向調査（2008 年下期）7 ダークネット観測の技術動向と観測事例，（オンライン），入手先 ⟨http://www.ipa.go.jp/security/fy20/reports/tech1-tg/2_07.html⟩（参照 2015-3-26）．
[3] 宮崎 桐果, 小刀稱知哉, 池部実, 吉田和幸：大分大学の未使用 IP アドレスに対する TCP/80 番ポートへの通信の解析，第 67 回電気・情報関係学会九州支部連合大会，pp. 89–89 (2014 年 9 月)．
[4] 佐藤聡, 三田尚貴, 新城靖, 板野肯三：ハニーポットを利用した筑波大学の未使用 IP アドレス宛ての HTTP リクエストの解析，情報処理学会研究報告 (インターネットと運用技術)，Vol. 2013-IOT-23(8), pp. 1–6 (2013 年 9 月)．
[5] 金高一, 松井一乃, 加来麻友美, 池部実, 吉田和幸：ハニーポットを用いたアドレスハーベスタと spam 送信者の spam 活動の調査，情報処理学会第 6 回インターネットと運用技術シンポジウム (IOTS)2013 論文集，pp. 25–32 (2013 年 12 月)．
[6] 小刀祢知哉, 天本大地, 池部実, 吉田和幸：scan 攻撃検知システムを用いた被検知ホストの挙動についての調査，第 65 回電気関係学会九州支部連合大会，pp. 278–278 (2012 年 9 月)．
[7] Minoru Ikebe and Kazuyuki Yoshida: An Integrated Distributed Log Management System with Metadata for Network Operation, *The 7th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS 2013), 5th International Workshop on Virtual Environment and Network-Oriented Applications (VENOA2013)*, pp. 747–750 (2013).