Vol.2013-IOT-23 No.8
2013/9/27

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

佐藤 聡[1,a)]　三田 尚貴[2,†1]　新城 靖[3]　板野 肯三[3]

概要：筑波大学に割り当てられている IP アドレスの中で運用していないセグメント宛の通信は運用上破棄していた．この破棄されたパケットのうち TCP/80 番ポート宛のパケットをハニーポットにて処理することにより，筑波大学の IP アドレス内に設置されている Web サーバにどのような攻撃があるかの解析を行ったのでその結果を報告する．

キーワード：ハニーポット，ネットワーク解析，大学ネットワーク運用

Analysis of HTTP request to IP addresses which not assigned in University of Tsukuba using a honeypod

Abstract: Packets to IP addresses which are not used in University of Tsukuba was dropped at campus-central routers for normal operation. Among these dropped packets, The packets to TCP/80 port are processed with a honeypot. And we analyzed what kind of trend for unsuitable access to servers with the IP address of University of Tsukuba is. In this paper, we report the results of analysis.

Keywords: honeypod, network analysis, campus network operation

1. はじめに

現在，筑波大学には，IP アドレスとしてクラス B の領域が 2 つ割り当てられている．筑波大学において IP アドレスは有効的に利用されているが，それでも未使用の IP アドレスの領域が存在している．これらの利用されていない IP アドレス領域宛のパケットが筑波大学内部にあるルータに到着すると，そのルータではデフォルトルートが大学の境界に設置されているファイアウォールに向けられているため，ルータとファイアウォールの間で何度も送受信が行われてしまう．そのため，未使用の IP アドレス領域宛のパケットは内部のルータにて破棄している．利用されていない IP アドレス宛のパケットであるため，破棄してしまっても問題はない．しかしながら，相当量のパケットを破棄してしまっている．これらの破棄しているパケットの有効利用を考える．たとえば，使われていない IP アドレス宛への通信は攻撃である可能性があるため，それらのパケットを解析することにより攻撃の早期発見ができるかもしれない．

廣津らの研究 [8] では，攻撃的なトラフィックの解析のために，このように未使用の IP アドレス空間のおけるトラフィックを解析していた．これらの未使用の IP アドレス空間に対するトラフィックの場合，それらの含む IP アドレス空間がどのような組織に割り当てられているかによって，トラフィックの傾向が異なっている可能性もある．また，それらの研究では，パケットを対象にして解析を行っていた．それらの研究では，攻撃性のあるトラフィックは特定のアドレス空間での偏りがあり，またトラフィックの集中が起こるのは半日から 1 日以上の期間であることがわ

[1] 筑波大学 学術情報メディアセンター
Academic Computing and Communications Center, University of Tsukuba
[2] 筑波大学 情報学群情報科学類
College of Information Science, The School of Informatics, University of Tsukuba
[3] 筑波大学 システム情報工学域 情報工学域
Division of Information Engineering, Faculty of Engineering, Information and Systems, University of Tsukuba
[†1] 現在，東京大学工学系研究科システム創成学専攻
Presently with Department of System Innovation, School of Engineering, The University of Tokyo
[a)] akira@cc.tsukuba.ac.jp

かった．

しかし，プロトコルベースではどのような通信が行われているかの解析は行われていない．特に，近年，最も頻繁に使われている HTTP を用いて，未使用 IP アドレス宛てにどのような通信を行っているかについての収集や解析は行われていない．HTTP は，膨大な Web ページの転送に利用されているだけでなく，HTTP 上で様々なプロトコルが動いている．そのため，HTTP サーバを対象にした攻撃も頻繁に行われるようになっている．したがって，HTTP による攻撃の傾向を把握することは非常に重要である．

また，筑波大学の未使用の IP アドレスに対してどのような通信が行われているかの解析は今まで行われていない．筑波大学の内部で廃棄されているパケットについては，境界のファイアウォールを通過してきている．このように組織の違いや，ファイアウォールを適用している場合の違いなどについての研究を行うことも大変重要である．

そこで，本研究では，未使用 IP アドレス宛ての通信をハニーポットで収集し，解析することを目的とした．特にその中でも，HTTP による通信を対象に収集を行い，解析を行った．本研究では，ハニーポットソフトウェアとして，honeyd [4] を用いた．この honeyd により，TCP/80 番ポート宛の通信に対して，HTTP の疑似的な応答を行うこととし，その際の HTTP におけるリクエストを収集した．TCP/80 番ポート宛の通信はすべて HTTP を用いているとは限らないため，HTTP の規約に即さない場合の通信についても，可能な限りの情報を収集した．

収集した情報をもとに HTTP リクエストの解析を行った．収集を行った期間において，open proxy の探索を行っていると思われる通信や，複数の IP アドレスが協調して送信しているリクエスト，さらに phpMyAdmin の脆弱性を狙った攻撃と思われるアクセスを発見することができた．

2. 関連研究

2.1 未使用のアドレス空間におけるトラフィックの解析

2.1.1 分散協調ネットワークの監視

廣津らの研究 [8] では，ネットワーク上を流れる攻撃性トラフィックの解析を行うために，複数の組織に割り当てられているネットワークのアドレス空間の一部を利用している．これにより，全体として広いアドレス空間の攻撃性トラフィックの監視に利用することにより，攻撃の傾向をより明らかにできる．廣津らの研究では，主に送信先 IP アドレスやポート番号，TCP コネクションにおける SYN や ACK パケットそれぞれの相関関係の解析を行い，攻撃性トラフィックの傾向を示している．

本研究では，筑波大学のネットワークの使用されていないセグメントを利用し，トラフィックの収集を行なっている．本研究は HTTP リクエストを収集し，解析することを目的としている．これにより，送信先 IP アドレスやポート番号のみではわからない傾向を把握することができると考えられる．

2.1.2 出現頻度の低い攻撃パターンの解析

福島らの研究 [6] では，同様にネットワークにおける使用されていないアドレス空間を利用してトラフィックの収集を行なっている．そこで福島らは，長期間にわたって少しのパケットしか送信をしないような気付かれにくい攻撃の検知手法を提案している．この手法により，総トラフィック量のうち数 %という僅かな攻撃の傾向を抽出することに成功している．

本研究では，HTTP リクエストに基づく攻撃パターンの収集を目的としている．また，攻撃パターンを収集する際，HTTP リクエストが送られる間隔がある一定時間以上の通信は攻撃パターンの一部とみなさず，新しいパターンとして収集している．

2.1.3 中京大学における調査

長谷川の研究 [9] では，中京大学に設置されたハニーポットによるウェブアクセスを調査している．この調査では，ハニーポットは 1 つの IP アドレスに対する通信を対象としている．本研究では，複数かつ大量の IP アドレスに対する通信を対象としているため，アクセス元が多数のアクセス先に通信している際にどのような通信を行っているが観測可能である．なお本研究でも一部においては，長谷川の研究にて報告されているアクセス傾向と同じものが観測されている．

2.2 NIDS とハニーポットを組み合わせたシステムの提案

比嘉らの研究 [7] では，オープンソースソフトウェアの IDS(In trusion Detection System) と honeyd を組み合わせ，初心者でも導入，運用が可能な不正侵入防止システムの提案をしている．このシステムでは，IDS と honeyd それぞれでログ情報の取得を行う．そして，IDS で検知されなかった不正通信を検知するために honeyd を使用し，iptables[5] を使いパケットフィルタリングを行う．これにより，IDS で対応することができなかった不正通信に対しても honeyd を利用し，ネットワークの保護が可能となる．

本研究では，IDS を用いたパケットフィルタリング [1] などを行わない．しかし，HTTP に関してスクリプトを利用し，筑波大学のネットワークにおける不正な通信について HTTP リクエストの攻撃パターンの収集を行う．

3. 収集方法

3.1 筑波大学のネットワーク環境

本研究では，筑波大学のネットワークにハニーポットを設置して攻撃情報を収集する．筑波大学のネットワークは 130.158.0.0/16 と 133.51.0.0/16 とのクラス B の 2 つの IP アドレスが割り当てられている．学内では，所有している

IP アドレスをさらに小さいサブネットに分けて利用している．そのため，利用されていないサブネットが存在する．そのサブネット宛の通信は原則として不適切な通信である．

なお，これらの IP アドレスは論理的には，学内と学内の境界にあるファイアウォールに内側に接続されている．したがって，学外からこれらの IP アドレスにアクセスは，ファイアウォールによる制限を受けている．筑波大学では，ファイアウォールは，学外から学内への TCP/80 番ポートへのアクセスは許可している．

3.2 honeyd の設置

本研究では，honeyd を内部のルータへ接続する．さらに，honeyd は，上記の 2 つのクラス B のネットワーク宛の通信であれば応答するように設定する．さらに，内部のルータのルーティングテーブルに対して筑波大学に割り当てられている 2 つのクラス B のネットワークへの next hop として honeyd の IP アドレスを設定する．内部のルータは，最長一致の方式によりルーティングを決定するため，利用されているサブネットは，2 つのクラス B のネットワークよりもネットマスクが長くなるために，正しいルーティングが行われる．使われていないサブネットに対しては，設定したルーティングが用いれるため，結果として学内ネットワークにおいて利用されていないサブネット宛の通信は honeyd に送られる．これにより，honeyd は，それらの通信を監視することが可能になる．

3.3 取得する情報

本研究では利用されていないサブネットの IP アドレスの TCP/80 番ポート宛のすべての HTTP リクエストとそれに対する応答を収集し，TCP/80 番ポート宛以外のパケットについては収集しない．

honeyd は各プロトコルにおいて疑似応答するプログラムをユーザが指定できる．またどのポート宛のパケットをどの疑似応答プログラムに転送するかも指定できる．本研究では TCP/80 番ポート宛のパケットのみを次節にて説明する疑似応答するプログラムに転送する設定を行った．

3.4 HTTP における疑似応答

本研究では，HTTP プログラムに疑似応答するプログラムを設計した．そのプログラムの設計方針は，送信元からの様々なリクエストに対して以下のような応答をするものとした．

(1) index ページに対する GET メソッドによる要求に関しては Apatch の初期ページを返す．
(2) それ以外のページに対する GET メソッドによる要求には，400 Bad Request を返す．
(3) HEAD メソッドによる要求には，200 OK を返す．
(4) 上記以外のメソッドによる要求には，501 Not Implemented を返す．

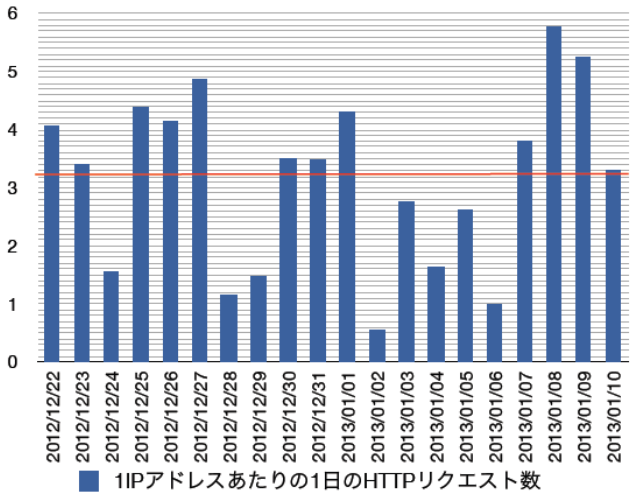

図 1 1 サーバあたりの平均アクセス数
Fig. 1 The average of accesses per one server

なお，送信元によっては HTTP に則らない通信を行う場合もあるため，HTTP に則らない場合には，一定時間新たな送信が来ないことを確認した後，コネクションを切断する様にした．

上記のいずれの対応においても，HTTP のリクエストラインとヘッダ情報とともに，通信の開始時刻，送信元 IP アドレス，送信元ポート番号，送信先 IP アドレスも収集した．収集した情報はデータベースに格納した．

4. 解析結果

本章では，収集した情報をもとに分析を行った結果を示す．なお，本研究において，HTTP リクエストの送信元をホスト，送信先をサーバと呼ぶことにする．

4.1 概要

本研究では，2012 年 12 月 22 日から 2013 年 1 月 10 日までの期間について収集を行った．この期間において筑波大学にて利用していない IP アドレスの総数は 73,728 件であった．この期間において honeyd の TCP/80 番ポートにアクセスがあった件数の合計は，5,203,287 件であった．したがって 1 サーバ・1 日当たりの平均アクセス数は 3.21 件であった．**図 1** に収集期間内の一日ごとの 1 サーバあたりの平均アクセス数を示す．図中の赤い線は収集期間内の 1 サーバ・1 日当たりの平均アクセス数を表す．図 1 よりアクセス数の日ごとの変化について曜日などの周期性はない．

4.2 HTTP リクエストの解析

honeyd が受け取った HTTP リクエストの内容 (総数:5,203,287 件) についての解析を行った．まずリクエストを HTTP に則っているリクエストと HTTP に則っていないリクエストの大きく 2 種類に分類したところ，それ

表 1　リクエストの分類ごとのアクセス数の割合
Table 1　The rate of the number of accesses for every classification of a request

分類	割合
HTTP に則っているもの	(小計)42%
1) GET http:// から始まるもの	18%
2) script/setup.php を含むもの	10%
3) HEAD メソッド	5%
4) GET メソッドによる index の取得	3%
5) その他の GET メソッド	5%
6) その他のメソッド	1%
HTTP に則っていないもの	(小計)58%
1) ASCII 制御文字列 1	24%
2) ASCII 制御文字列 2	12%
3) ASCII 制御文字列 3	12%
4) リクエストラインが空	8%
5) BitTorrent	2%
6) その他	0%

ぞれの割合は 42%と 58% になった．さらにそれら各々を分類し，その分類ごとの総数を数えた．分類ごとの割合を**表 1** に示す．

この分類において特に割合が大きい，GET http://で始まるリクエスト，scripts/setup.php を含むリクエストについて詳細に調査した．

4.2.1　GET http://で始まるリクエスト

頻出したリクエストの上位 3 件を**表 2** に表す．

これらの GET http:// で始まるリクエスト群を送信するホストは，おそらく open proxy の探索を行なっているものと思われる．

GET http://gameframe.net/headers HTTP/1.1 と GET http://www.yahoo.co.jp HTTP/1.1 は少数のホストが多数のサーバへとアクセスしていることがわかる．

また，GET http://www.baidu.com/ HTTP/1.1 を送るホストにおいて，上位 24 ビットが一致しており，連続である IP アドレスであることが確認された．これらは，それぞれの IP アドレスが協調してリクエストを送信していると考えられる．

4.2.2　scripts/setup.php を含むリクエスト

phpMyAdmin の脆弱性を狙った攻撃と思われるアクセスがあった．phpMyAdmin とは，MySQL サーバを Web ブラウザから管理するためのデータベース接続クライアントであり，PHP にて実装されている [3]．これには，いくつかの脆弱性があることが報告されている [2]．今回，発見したリクエストラインには，script/setup.php という phpMyAdmin における，設定を行うスクリプトの名前となる文字列にも含まれている文字列である．これらのリクエスト群の各々について，ホスト数，サーバ数，件数，リクエストの総数に対する割合を**表 3** に表す．

表 3 より，少数のホストが 9 種類のリクエストを多数のサーバに送信していることがわかる．また，これらの HTTP リクエストがどのように送信をされているかを調査したところ，以下のような特徴がみられた．

- 同じサーバに対して，連続的にリクエストを送信しているホストはない
- あるホストは，以下のようにアクセスを行う
  (1) あるひと塊の IP アドレスをもつサーバ群に，1 種類のリクエストでアクセスを行う
  (2) 同じ塊の IP アドレスをもつサーバ群に，異なる 1 種類のリクエストで再びアクセスを行う
  (3) (2) を複数回行い，その後，他の塊に対して，上記 (1),(2) を行う

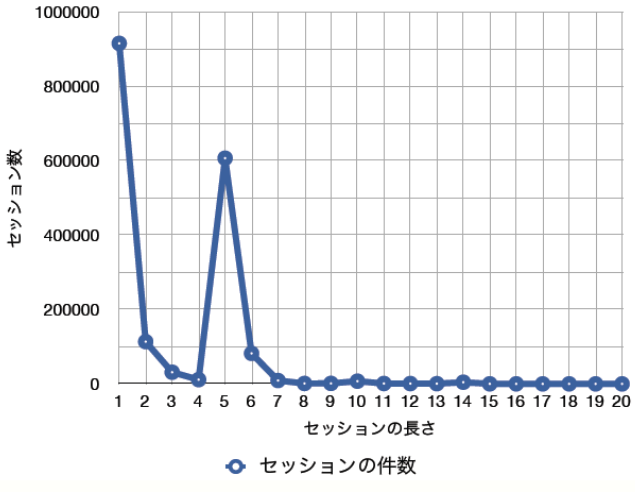

図 2　セッションの長さと総数
Fig. 2　The length and total number of sessions

4.3　HTTP リクエストのセッション解析

本研究では，1 つのホストが 1 つのサーバに対して，どのように HTTP リクエストを送信したかに注目した．そこで，HTTP リクエストを詳細に解析するために，セッションという概念を用いる．セッションとは，1 日 (24 時間) という期間内において 1 つのホストと 1 つのサーバを 1 組としたものである．また，1 セッション中に送られた HTTP リクエストの数を長さとする．

図 2 は横軸をセッションの長さ，縦軸をセッション数としたグラフである．本来，セッションの長さが長くなるにつれて，セッション数が減少していくと考えられるが，長さが 5 および，6 の時，セッション数が非常に多くなっていることがわかる．本研究では，長さが 1，2，5，6 の時のセッションについての調査を行った．

4.3.1　長さが 1 のセッション

頻出したセッションの上位 3 件を**表 4** に表す．表 4 において，セッションが (空) と記載してある場合はリクエストラインが送られていないことを表す．表 4 の上位 2 件のセッションは多数のホストと多数のサーバの組である

表 2 GET http:// で始まるリクエストにおいて頻出するリクエスト (上位 3 件)
Table 2 The request which starts by 'GET HTTP://' occur frequently (top 3)

HTTP リクエスト	ホスト数	サーバ数	件数	割合
GET http://gameframe.net/headers HTTP/1.1	2	48,276	633,475	78.4%
GET http://www.baidu.com/ HTTP/1.1	183	53,723	146,500	18.1%
GET http://www.yahoo.co.jp HTTP/1.1	1	41,196	41,196	5.1%

表 3 script/setup.php を含むリクエストにおいて頻出するリクエスト
Table 3 The request which includes 'script/setup.php' occur frequently

HTTP リクエスト	ホスト数	サーバ数	件数	割合
GET /phpMyAdmin/scripts/setup.php HTTP/1.1	9	60,683	205,602	38.9%
GET /myadmin/scripts/setup.php HTTP/1.1	8	56,020	154,650	29.2%
GET /pma/scripts/setup.php HTTP/1.1	9	59,481	101,609	19.2%
GET /admin/scripts/setup.php HTTP/1.1	3	29,501	30,275	5.7%
GET /mysql/scripts/setup.php HTTP/1.1	1	22,679	22,680	4.3%
GET /admin/pma/scripts/setup.php HTTP/1.1	2	6,179	6,956	1.3%
GET /admin/phpmyadmin/scripts/setup.php HTTP/1.1	2	6,167	6,952	1.3%
GET //phpMyAdmin//scripts/setup.php HTTP/1.1	1	5	10	0.0%
GET ///scripts/setup.php HTTP/1.1	1	5	5	0.0%

表 4 長さ 1 のセッションにおける頻出するセッション (上位 3 件)
Table 4 The session which of lenght is 1 occur frequently (top 3)

セッション	件数	割合
(空)	280,973	30.7%
HEAD / HTTP/1.0	253,123	27.6%
GET http://www.baidu.com/ HTTP/1.1	109,099	11.9%

表 5 長さ 2 のセッションにおける頻出するセッション (上位 3 件)
Table 5 The session which of lenght is 2 occur frequently (top 3)

セッション	件数	割合
GET / HTTP/1.1 GET http://www.yahoo.co.jp HTTP/1.1	40,960	36.1%
(空) (空)	12,121	10.1%
GET / HTTP/1.1 GET /robots.txt HTTP/1.1	11,021	9.7%

表 6 長さ 5 のセッションにおける頻出するセッション (上位 1 件)
Table 6 The session which of lenght is 5 occur frequently (top 1)

セッション	件数	割合
00 (ASCII 制御文字列 2) GET http://gameframe.net/headers HTTP/1.1 04 01 00 (ASCII 制御文字列 3) 05 01 00 (ASCII 制御文字列 1) 05 01 00 (ASCII 制御文字列 1)	591,933	98.4%

ことが確認された．また，GET http://www.baidu.com/ HTTP/1.1 は表 2 にて報告した 頻出するリクエストに含まれている．長さ 1 に含まれる数はそのリクエストの総数の約 75%であった．

4.3.2 長さが 2 のセッション

頻出したセッションの上位 3 件を**表 5** に表す．表 5 において，(空) (空) となっているセッションはリクエストラインが空である HTTP リクエストが 2 つ送られていることを表している．

表 5 において，割合が最も多いセッションにて送られている GET http://www.yahoo.co.jp HTTP/1.1 というリクエストは，表 2 に示しているリクエストである．表 2 に示した当該リクエストの 99%以上がこのセッションにて送られている．このセッションがどのように送信されているか調査したところ，1 つのホストが複数のサーバに対して，連続的にこのセッションを送信していることがわかった．このことから，このセッションでは，GET / HTTP/1.1 のリクエストを送信して，web サーバの存在を確認した後，GET http://www.yahoo.co.jp HTTP/1.1 を送信することより，open proxy の探索を行なっているものと考えられる．

次に，表 5 において，割合が 2 番目に多いセッションに含まれる，リクエストラインが空である HTTP リクエストは短い期間に多数のホストに送られている．従って，このセッションはあるサーバ群に対して，1 日より短い期間でアクセスをした結果，長さ 2 のセッションとなった可能性も考えられる．

最後に，GET /robots.txt HTTP/1.1 を送るセッションは検索ロボットであることが考えられる．通常，検索ロ

表 7　長さ 6 のセッションにおける頻出するセッション (上位 1 件)
Table 7　The session which of lenght is 6 occur frequently (top 1)

セッション	件数	割合
GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1 GET /phpMyAdmin/scripts/setup.php HTTP/1.1 GET /phpmyadmin/scripts/setup.php HTTP/1.1 GET /pma/scripts/setup.php HTTP/1.1 GET /myadmin/scripts/setup.php HTTP/1.1 GET /MyAdmin/scripts/setup.php HTTP/1.1	57,969	70.6%

ボットは，あるサーバに対してルートディレクトリの取得 (GET / HTTP/1.1 リクエストの送信) を行った後に，同じサーバに対して robots.txt の取得を行なっているからである．また，このセッションはある特定のサーバが集中してセッションを受け取っているということではなく，少数のホストが多数のサーバに対してアクセスを行なっている，すなわち，ネットワークの一部のサーバ群に対して，まんべんなくアクセスを行なっているといえる．

4.3.3　長さ 5 のセッション

長さ 5 のセッションを調べたところ，**表 6** に示す通り，1 種類のセッションがの 98%以上を占めていることがわかった．このセッションでは 05 01 00(ASCII 制御文字列 1)，00(ASCII 制御文字列 2)，04 01 00(ASCII 制御文字列 3) といった制御文字列を送っていることから，通常は HTTP が使う TCP/80 番ポートを使って異なるプロトコルにより通信を行おうとしている可能性が考えられる．どういったプロトコルであるかの解析は今後の課題である．

4.3.4　長さ 6 のセッション

長さ 6 のセッションを調べたところ，表 3 にて示したリクエストが含まれている．4.2.2 節にて述べたように，このセッションは，1 つのホストが 1 つのサーバへ連続してリクエストを送信しているということではなく，特定のひと塊の IP アドレスを持つサーバ群に対して，異なるリクエストを 1 種類ずつ送信した結果である．

5.　おわりに

本研究では，筑波大学のネットワークにおける未使用 IP アドレスを利用し，HTTP リクエストの収集を行い，収集した情報を元に解析を行った．特に，送信者が同じ IP アドレスに対して，送信する HTTP リクエストのセッションについて着目し，送信者の通信の振る舞いを解析した．

リクエストラインの内容に応じて，HTTP リクエストを複数に分類し，占める割合が多いものについて調査を行った．また，収集した HTTP リクエストに関して，セッションという概念を利用した解析を行った．中でも，長さが 1,2 のセッション，およびセッション数が特異であった長さが 5,6 のセッションについて調査した．これらから，web サーバの存在を確認した後，GET http://から始まるリクエストを送信しているものなどがみられた．また，phpMyAdmin の脆弱性を狙った攻撃と思われるアクセスを多数確認でき，かつその攻撃パターンも明らかになった．HTTP ではないがいくつかのサーバに同じパターンでアクセスするセッションも確認できた．

今後の課題は，よりよい分析を得るためのセッション区切る方法の開発があるまた，SMTP 等の他のプロトコルと対象とした収集分析も行う必要がある．

参考文献

[1] Khosravifar, B. and Bentahar, J.: An Experience Improving Intrusion Detection Systems False Alarm Ratio by Using Honeypot, *Advanced Information Networking and Applications, International Conference on*, Vol. 0, pp. 997–1004 (online), DOI: http://doi.ieeecomputersociety.org/10.1109/AINA.2008.44 (2008).

[2] National Vulnerability Database: Vulnerability Summary for CVE-2010-3055, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3055. 2013 年 1 月 23 日閲覧.

[3] phpMyAdmin devel team: phpMyAdmin, http://www.phpmyadmin.net/. 2013 年 1 月 23 日閲覧.

[4] Provos, N.: A virtual honeypot framework, *Proceedings of the 13th USENIX security symposium* (2004).

[5] The Netfilter webmaster: iptables, http://www.netfilter.org/projects/iptables/. 2013 年 1 月 16 日閲覧.

[6] 福島祥郎，堀　良彰，櫻井幸一：ダークネット観測データに基づく攻撃挙動の特徴抽出に関する考察，電子情報通信学会技術研究報告. ICSS, 情報通信システムセキュリティ， Vol. 109, No. 285, pp. 37–42（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110007520923/⟩ (2009).

[7] 比嘉哲也，長田智和，谷口祐治，玉城史朗：NIDS とハニーポットを組み合わせた不正侵入防止システムの開発，電子情報通信学会技術研究報告, 情報ネットワーク研究会， Vol. 109, No. 411, pp. 1–4（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110008000298/⟩ (2010).

[8] 廣津登志夫，福田健介，栗原　聡，明石　修，菅原俊治：断片アドレスを用いた分散協調インターネット監視に関する一考察 (OS-2：セキュリティ)，情報処理学会研究報告. [システムソフトウェアとオペレーティング・システム]， Vol. 2007, No. 83, pp. 39–45（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110006390000/⟩ (2007).

[9] 長谷川明生：単純なハニーポットによるウエブアクセス動向調査，情報処理学会研究報告インターネットと運用技術（IOT），Vol. 2013-IOT-20, No. 17, pp. 1–4 (2013).