HTTP通信ログ解析による学内情報機器の利用状況推定

鳩野 逸生[1,a)]

概要：神戸大学では, 学外向けの HTTP 通信のログ情報を, 発信元および送信先 IP, URL, User Agent 情報を含んだ形で, 2012 年から取得して記録している．Web ブラウザなどが発生する HTTP リクエストに含まれる User Agent 情報には，ブラウザ名，バージョン，オペレーティングシステムなどが含まれており，解析することで発信元の PC で利用しているオペレーティングシステム等の情報を推定できる可能性がある．本稿では，HTTP 通信ログ情報に含まれる User Agent 情報および HTTP リクエストの URL を解析することにより，発信元 IP に接続されている PC などの情報機器で利用されているオペレーティングシステムやブラウザの利用状況を IP 毎に集計する機能の概要について述べる．本機能は，学内ネットワークに接続された情報機器の状況を調査することを目的として開発したものである．さらに，得られた集計結果を Windows XP を利用した PC の状況, モバイル機器の利用状況の把握等に適用した事例について述べる．

Estimation of Usage Situation of Software on PCs in a University Based on Analysis of HTTP Logging Information

Itsuo Hatono[1,a)]

Abstract: This paper deals with estimation of usage situation of software on PCs connected to the campus network in Kobe University based on the analysis of HTTP logging information. In Kobe University, HTTP logging information, which includes source and destination IP, URL, User Agent, and so on, has been collected and stored from 2012. Since user agent information includes various information about the software, which generate the HTTP requests, operating systems and so on, we can estimate the software and the operation system in each PC. In this paper, we describe the analysis program of HTTP logging information in order to estimate the usage situation of PCs. Furthermore, we also describe the case of finding PCs installed Windows XP in Kobe University.

1. はじめに

近年，セキュリティ修正に関するサポートが打ち切られたオペレーティングシステム (以下，OS とする) やソフトウェアへの対処が問題となっている．2014 年 4 月に Microsoft 社 Windows XP サポートが終了した際に大きな社会的な話題になったことが典型的な例としてあげられる [1].

このような状況の下で Windows XP のリプレース促進に有効な対策を講じるためには，各 PC で用いられているオペレーティングシステムや Web ブラウザ等の基本的なソフトウェアの利用状況を把握することが必要である．利用状況の把握には，利用者・管理者へのアンケートやソフトウェア管理を行うためのソフトウェアを導入することが考えられる．しかし，大規模な大学の研究室に設置されている PC に対して前述の方法で利用状況を調査することは，人的・金銭的コストや網羅性・正確性などの点で問題が大きいため，実施することは困難であると予想される．

神戸大学においては，インシデント発生時の調査や不正利用の監査を主な目的として，学内から学外への HTTP 通信のログ情報を取得し，保存している．これは, 神戸大学における情報セキュリティポリシーにおいて，基幹ネットワーク管理者は，学内のセキュリティ状況を把握してセキュリティ維持のための施策をとる必要がある，という規

[1] 神戸大学 情報基盤センター
Information Science and Technology Center, 1-1 Rokko-dai, Nada, Kobe 657-8501 Japan
[a)] hatono@kobe-u.ac.jp

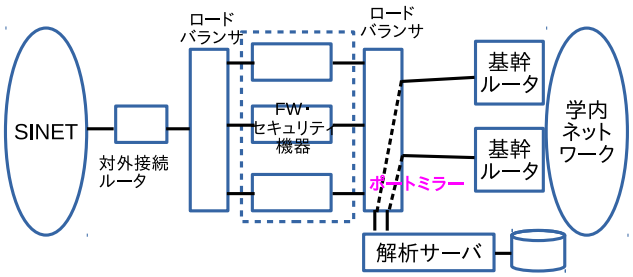


図 1 HTTP 通信取得の取得位置

定を根拠に実施しているものである [*1].

取得しているログ情報は，発信元 IP, 送信先 IP, HTTP Method, URL, Referer, User-Agent などを含んでいる．特に User-Agent 情報は，多くの場合 HTTP 通信を行うソフトウェアや OS に関する情報が含まれていることから，User-Agent 情報を各 IP 毎に分析して蓄積することにより IP 配下に接続された PC の利用状況を推定できるのではないかと考えられる．通信をモニタし，通信パケットにおける fingerprint を観測して接続機器のオペレーティングシステムや利用アプリケーションを推定して出力する高機能なファイアウオール機器も発表されている (例えば [2]) が，高速でかつ大規模なネットワーク全体を把握するためには，高額な機器が必要であり，現状では導入することは難しい．

本稿では，Windows XP のサポート終了対応を期に開始した，IP 毎の User-Agent 情報の解析・蓄積とその利用事例について述べる．

2. HTTP 通信情報の取得

2.1 HTTP 通信取得位置

学内のすべての HTTP 通信を記録することは現実的ではないため，学内からの通信がファイアウオールを通る直前に設置しているロードバランサのポートをミラーし，それらのポートを解析サーバから通信モニタリングソフトウェア tshark[3] を用いることにより HTTP 通信ログを取得している (**図 1**)．基幹ルータからロードバランサは 10Gbps で接続されているが，ミラーポートは 1Gbps であることと，解析サーバの性能を考慮するとかなりのパケットを取りこぼしていることが予想される．しかし，100%すべてのパケットを取得するためにはかなりのコストがかかるため本構成としている．

2.2 tshark による HTTP 通信の取得

図 1 に対して，tshark のプロトコル解析機能を用いて，時刻，ソース IP, 相手先 IP, HTTP request method, ホスト名， URI, HTTP request version, Content Length, Referer, User_Agent, ソースポート, 相手先ポートを取得して, apache HTTP server における combined access_log フォーマット [4] に近い形に整形してファイルに出力している．本通信の取得においては，通信パケットをモニタして取得している関係上，HTTP リクエスト と サーバレスポンスは, 異なったパケットとして観測される．厳密に combined access_log フォーマットに変換するためには，一連の HTTP リクエストに対するサーバレスポンスをすべて関係付ける必要がある．しかし，前述のように本物理構成ではパケットがすべて取得できているとは限らず，すべてを関連付けることは困難であると予想されるため，HTTP リクエストとサーバレスポンスに対する関連付け処理は行っていない [*2].

3. HTTP ログ情報の解析

HTTP ログ情報の解析にあたっては，User-Agent 情報の解析にあたっては，以下の仮定をおいている．

(1) Web ブラウザ等, HTTP 通信を発生させるプログラムが生成する HTTP リクエストにつけられる User-Agent 情報には，ブラウザの種類, バージョン, OS の種類，OS のバージョンに関する情報が含まれる [*3].
(2) モバイル機器等が生成する HTTP リクエストに関しては，ハードウェアの種別等に関する情報が含まれる．
(3) 主要なウイルス対策ソフトがパターンファイルのチェック/ダウンロードに使用する HTTP リクエストにつけられる User-Agent は, ユーザ情報と思われる英数字のパターンがつけられる場合がある．

また，ブラウザ以外のソフトウェアが生成する HTTP リクエストに対しては以下の経験的な知識を適用している．

(1) アップデートの自動チェックを行う多くのソフトウェアでは，更新のチェックおよびダウンロードの際にほぼ定形とみなせる URL に対してアクセスを行う．ただし，Microsoft 社が販売/提供しているウイルス対策ソフトのパターンチェック・更新は, Windows update に対する通信の中に含まれるために判別していない．

以上のような仮定に基づき，以下のような情報を IP 毎に解析する．

Web ブラウザ等: Internet Exploler, Firefox, Chrome, SeaMonkey, Safari, Opera 等

OS およびバージョン: Windows, MacOS, Android, Linux 等

主要なウイルス対策ソフト利用状況: 主要なウイルス対策ソフトメーカ (Microsoft を除く)

User-Agent: 解析前の User-Agent 情報を 20 種類までは IP 毎に検出順に記録する．20 種類を超えた場合は,

[*1] この他に，sFlow を用いた通信パケットのサンプリングによる収集を実施している．

[*2] 取得したログに対して 1 日分 HTTP リクエストとサーバレスポンスを関連付けることを試みたところ, 20–30%関連付けることができなかったレコードが存在した．

[*3] Web ブラウザの他，メールソフトウェア，オフィスソフトウェアなども含まれる．

1)133.xx.yy.zz(2014 年 0831-0907) の状況

IP address 133.xx.yy.zz (Http カウント=95552)
Windows OS の状況
Windows NT 6.1: 検出 (1)
Windows Update の状況
Update 実行 (215)
Virus Scan ソフトのパターンファイル更新状況
virus:Kaspersky: 検出 (回数=85)
利用ブラウザバージョン等の状況
Brw:Chrome/36.0: 検出 (90996)
Brw:Firefox/28.0: 検出 (32)
Brw:Firefox/32.0: 検出 (7)
Brw:Firefox/9.0: 検出 (21)
Brw:Microsoft Office/14.0: 検出 (12)
Brw:Safari/534: 検出 (32)
Mac OS の状況
未検出
Mobile 機器の利用状況
未検出
Linux OS の状況
Linux:x86_64 unkown: 検出 (1)

観測したブラウザの User-Agent の状況 (20 のみ表示)

IPM
*[0-9A-Za-z%]{23,}-MAaHAAAAAAMAA=
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.143 Safari/537.36
Microsoft Office/14.0 (Windows NT 6.1; Microsoft Word 14.0.7128; Pro)
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/534.34 (KHTML, like Gecko) rekonq Safari/534.34
Mozilla/5.0
Mozilla/5.0 (X11; Linux x86_64; rv:9.0.1) [0-9A-Za-z]{5,}([+/]{1})[0-9A-Za-z]{5,} Firefox/9.0.1 SeaMonkey/2.6.1
*[0-9A-Za-z%]{23,}=
Windows([+/-][0-9A-Za-z]{5,})-Agent
*[0-9A-Za-z%]{23,}-FAaHAAAAAAMAA=
Microsoft([+/-][0-9A-Za-z]{5,})/6.1
Google Update/1.3.24.15;winhttp
Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17)
Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17),Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17),(略)
Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17),Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17)
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:32.0) [0-9A-Za-z]{5,}([+/]{1})[0-9A-Za-z]{5,} Firefox/32.0
Wget/1.10.2
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Mozilla/5.0 (X11; Linux x86_64; rv:28.0) [0-9A-Za-z]{5,}([+/]{1})[0-9A-Za-z]{5,} Firefox/28.0 SeaMonkey/2.25
Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17),Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17)(略)
Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17),Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17),(略)
Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17),Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17)(略)

図 2 各 IP 毎の解析結果出力例

図 3 IP 範囲・User Agent 内文字列検索指定インタフェース

Date	Avast	Avira	Eset	Kaspersky	Mcafee	Sophos	Symantec	Trendmicro	Windows NT 4.0	Windows NT 5.0	Windows NT 5.00	Windows NT 5.1	Windows NT 5.2	Windows NT 6.0	Windows NT 6.1	Windows NT 6.2	Windows NT 6.3	Windows NT 7.1	Windows NT 9.0
2013/1124-1201	6	76	326	80	74	105	1005	679	1	60	6	1752	30	451	3879	550	254	0	0
2013/1229-0105	0	30	109	32	23	33	381	249	0	29	2	549	19	173	1174	211	122	0	0
2014/0202-0209	1	79	336	88	27	133	933	678	0	60	3	1542	39	440	4005	742	385	1	1
2014/0309-0316	1	57	304	74	23	72	726	500	0	43	3	1175	36	272	3247	742	325	0	0

検出IP数 = 7102

図 4 集計情報の出力例

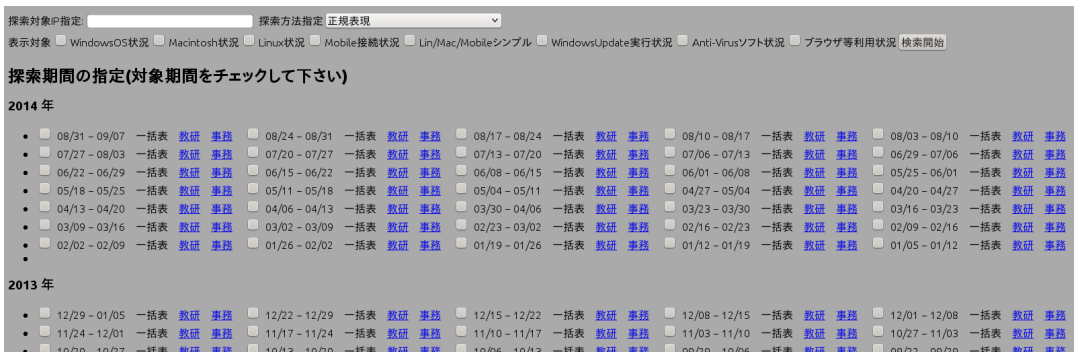


図 5 集計期間・IP 範囲の指定インタフェース

最初に検出したものから上書きしている．ただし，パターンが異なっていても同じソフトウェアから発生したものと判断できる場合は関しては，同じものとみなすことによりパターン数の限定を試みている．しかし，パターン数が限定できずパターン数が 1 つの IP から検出される数が非常に多くなる場合もある．このため，20 種類のみに制限することにより，記録に必要な容量を限定している．

以上のような解析を，1 週間に 1 回日曜日早朝に，バッチジョブで実行して保存している．対象とする IP は，神戸大学におけるユーザに割り当てられている全 IP を対象としているが，IP に対する接続 PC が動的に変わる全学無線 LAN サービスおよび VPN サービスに割り当てられたものは除いている．実際に解析処理を開始したのは，2013 年 10

月であるが，ログが残存していた 2012 年 10 月からの解析データを生成し，保存している．平日で，ログデータは約 3GB(gzip 圧縮) あり，2014 年 8 月 31 日から 9 月 7 日までのデータを処理するには約 5 時間要した．2012 年 10 月から 2014 年 8 月までのログデータの総容量は約 1.3TB となっている．

4. 解析情報出力例

解析情報の出力例を**図 2** に示す．画面には，指定された期間 (1 週間単位) における Windows OS の状況，Windows Update の実行の有無等が項目別に出力される. 画面例の IP には，Linux/Ubuntsu をルータとして，配下に ウイルス対策ソフトとして Kaspersky がインストールされた Windows 7 が OS としてインストールされた PC が接続されていることを確認している．表示対象の IP は, IP のレンジ指定および正規表現で指定することができる．また，保存された User Agent 文字列に対する文字列検索を行うこともできるインフェースを開発している (**図 3**).

さらに，観測 OS の情報やブラウザの情報は，集計情報として出力することができる．**図 4** に，Windows OS の検出状況とウイルス対策ソフト の利用状況の集計の出力例を示す．同表中の Windows NT 5.0/5.00, 5.1, 5.2, 6.0, 6.1, 6.2, 6.3 は，それぞれ，Windows 2000, XP, Server 2003, Server 2008, 7, 8, 8.1 に対応する (2 番目以降の Windows を省略している)．Windows NT 7.1 および Windows NT 9.0 と検出しているものに関しては対応する製品名は確認できなかった [*4]．集計表表示においては，**図 5** に示すインターフェースを用いて, 対象 IP 範囲，対象 (Windows/Mac/Linux/Mobile/ブラウザ種別等) を指定することができる．

5. 利用事例

5.1 Windows XP 利用 PC 把握に対する適用例

Windows XP のサポート停止は，2014 年 4 月以前数年前から社会的に問題視され対策が求められてきた．神戸大学においても，学内における Windows XP の利用状況に関する状況を，本ログ解析を用いて調査し，対策にあたってきた．

2011 年 11 月に第一回調査を実施した．解析にあたっては，本解析機能開発以前に作成した簡易のプログラムを利用し, 2011 年 11 月末の 1 週間分のログデータを用いて実施した．**表 1** に，2011 年 11 月当時の検出状況を示す．2011 年時点で Windows98 が検出されているが，詳細に調査すると一部のバージョンが古いウイルス対策ソフトが Windows98 という UserAgent を名乗って通信していることと，同 IP からバージョンが新しい Windows OS を検知していたことが判明した．以上のことから，2011 年 11 月の時点で Windows98 が実際に利用されていた可能性は低いと思われる．

表 1 2011 年当時の Windows OS 検出状況

	98	2000	XP	2003	VISTA	7	2010
検出数	161	96	2790	42	877	1825	2

以降, 対策には予算確保が必要であり，早期の連絡が必要であるという判断から，定期的に調査し，学内に通知し対策を依頼してきた．サポート終了直前の 2014 年 3 月には，本解析機能を用いて WindowsXP を検知した学内 IP の一覧を作成し，関連部署に配布して対策を依頼した．サポート終了後の 5 月に再び検出一覧を作成し, 学内に配布した．

図 6 に，2011 年から 2014 年 4 月現在までの Windows OS の利用状況の推移を, Windows OS を検知した数および比率で示す．Windows XP の比率が着実に減少していることから，Windows XP からの移行が進んでいたことが推察される．検出数が時期により大きく変位していることと，利用比率で 2014 年 1 月付近で大きく傾向が異なるデータなど，突然大きく検出台数が落ち込むデータがが出現しているのは，一週間の集計対象期間がすべて夏季・年末年始の休暇にかかり，稼働していた PC 自体が大幅に通常より少なかったためであると思われる．

5.2 Windows OS 検出の正確性に関する考察

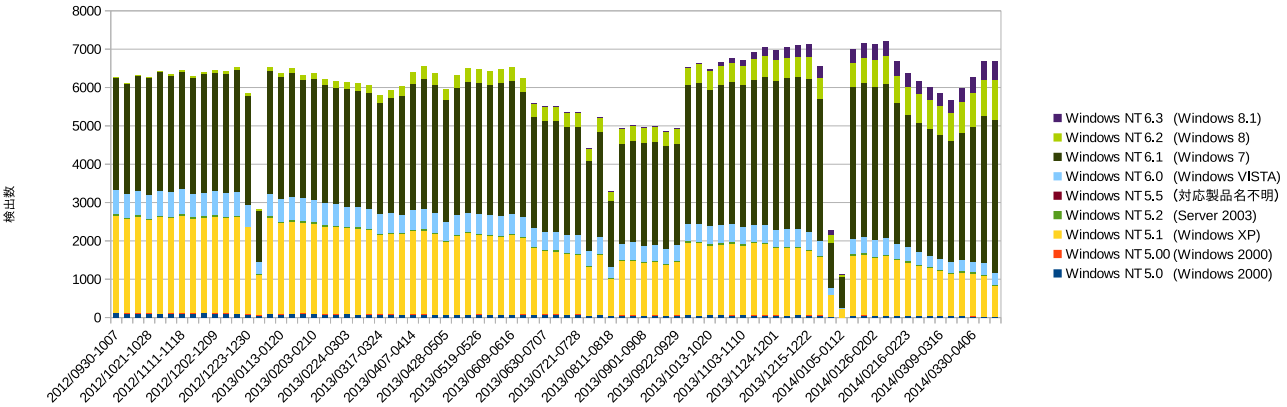
図 6 からわかるように，2014 年 4 月を過ぎてた時点でまた Windows XP が検出されている．神戸大学の情報セキュリティポリシー上は，サポート終了のオペレーティングの利用が禁止されていることから，学内に対象部署に警告を行ったが，該当の IP に Windows XP を利用した PC は接続していないという報告を受けたケースも見受けられた．このように，1 つの IP から Windows XP を含む複数の OS が検出されるという事象が発生するのは，

(1) 期間中に PC または OS の入れ替えを実施した．
(2) 該当 IP は NAT ルータが接続されており，プライベート側に Windows XP を含む PC が接続されている．
(3) Windows XP 以外の OS がインストールされているが，内部で動作しているプログラムが Windows XP という OS 名を User Agent に含めた形で通信を行っている．

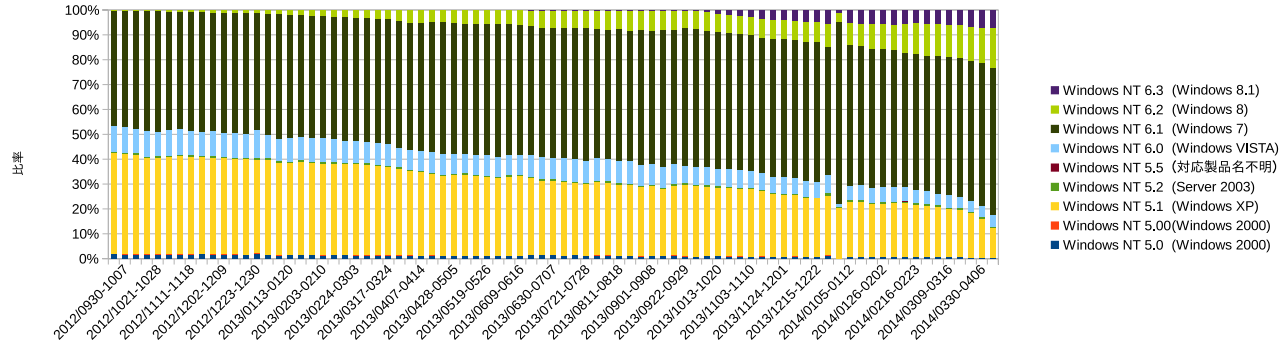
のいずれかであると考えられる．

検出の正確性を調査するため，NAT ルータによる接続が行われていないことが確認されているアドレスのレンジに関して, 2014 年 4 月 13 日から 20 日までのデータに関して調査を行った．アドレスレンジにおいて，753 個の IP を検出し，その中で 63 個の IP から XP を名乗る通信を検出したが，XP のみを検出した IP は 5 個であり，他の IP は

[*4] 検出数も僅かなことから誤検出の可能性が高い



(a) 各 Windows OS 利用台数の推移



(b) 各 Windows OS の利用率の推移

図 6 Windows OS 利用状況の推移

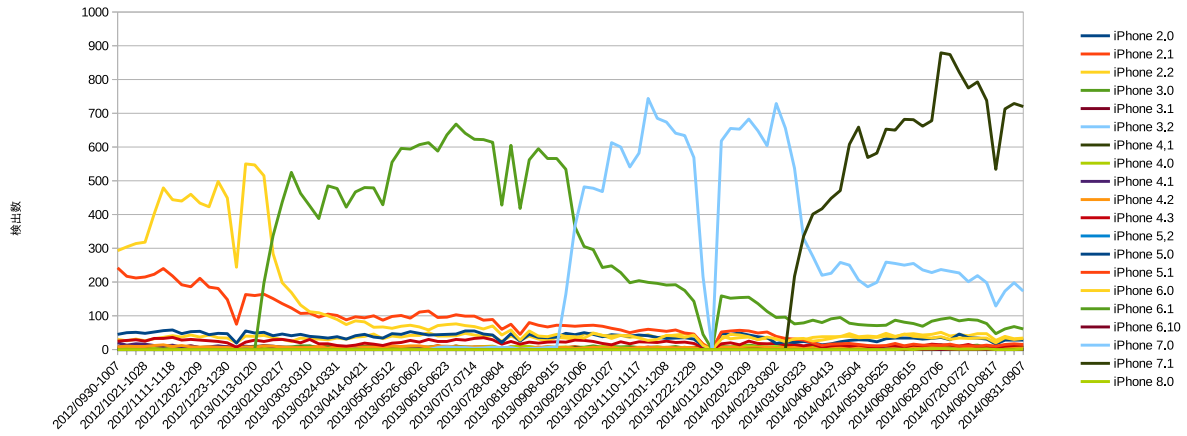
Windows 7 など別の Windows OS も同時に検出している．Windows XP 上のブラウザが，上位の OS の User Agent を用いることは考えにくいことから，実際にインストールされているのは Windows XP 以外に検出された OS であり，Windows XP を User Agent として利用している何らかの Web ブラウザ以外のプログラムが内部で動作しているものと思われる．この事例からは，2014 年 4 月時点で，IP と PC が一対一に対応している場合，Windows XP が検出された IP の 90%程度は誤検出であることが推察され，XP として検出された数より実際に XP が利用されている率はかなり低いものと思われる [*5]．

また，同一 IP レンジに対して，2012 年 11 月初旬一週間の解析データに対して同様の解析を実施した．その結果，Windows XP を検出した IP は 512 個であり，その中で Windows XP のみを検出した IP は 470 個であった．このことから，2012 年 11 月時点での誤検出率は約 10%であり，当時の検出数は Windows XP の利用数をかなり反映していたものと思われる．以上のことより，2014 年 4 月の時点で Windows XP と検出された PC の誤検出率が 90%であったという現象は，ブラウザ以外で Windows XP を名乗る通信を行うプログラムは，OS のバージョンを問わず一定率で存在しており，Windows XP を利用している PC の実数が 2014 年 4 月に入って大幅に減少し，相対的に誤差が大きくなったものと思われる．

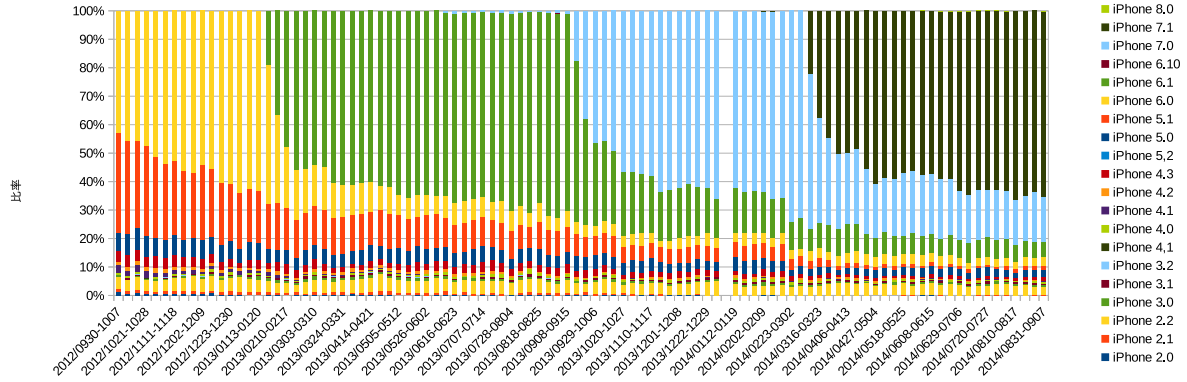
より正確な実数を把握するためには，複数のバージョンの Windows OS が検出された場合，最新バージョンを利用しているとみなす，という補正が必要であると考えられる．しかし，学内に数多く存在する NAT ルータ配下に複数台の PC が接続されている環境では，複数のバージョンが検出された場合，1 台の PC から発生したものか，実際に複数台異なったバージョンの OS を利用した PC が接続されているか区別することが困難なため，単純に前述の補正を適用することはできない．

しかし，本事例において必要な情報は，Windows XP の利用の傾向と接続されている可能性がある IP のリストアップであったため，詳細な解析・補正は実施しなかった．

[*5] このアドレスレンジは，比較的管理が厳重に行われていることが監査の結果判明しているレンジであるため，他のアドレスレンジにおける実 XP 検出率は 10%より高いと思われる．また，VMware 等のゲスト OS として XP が利用されていないことも判明している．



(a) iPhone における各 OS バージョンの検出数



(b) iPhone における各 OS バージョンの利用比率

図 7 iPhone における利用 OS の状況

5.3 誤検出 PC の詳細調査

2014 年 4 月に Windows XP が検出されたが，実際には別の OS が利用されていた中の一台について詳細な調査を実施した．基本的な利用状況は以下の通りである．

利用 OS: Windows 8
利用ブラウザ: Safari
Desktop： Bing Desktop

この PC に対応する送信元 IP の HTTP ログから，Windowsupdate，デスクトップ，Safari から送信される HTTP パケットに含まれている User Agent 情報から思われるログを除いた後に，“Windows NT 5.1” を User Agent として用いているログを抽出すると，User Agent として，以下の User Agent を含んだログが得られた．

```
compatible; MSIE 6.0; Windows NT 5.1; SV1
```

このアクセスは，HTTP GET リクエストではなく POST リクエストであり，毎朝起動時まもなく発生していたが，ログを過去に遡って調査すると，ある URL からフリーウェアをダウンロードした後に発生していた．該当 PC のユーザにインタビューしたところ，zip ファイルを解凍するソフトウェアをダウンロードしてインストールしたが，すぐに削除した，という答えを得た．この事実から，このフリーウェアをインストールした際に何らかのプログラムをバックグラウンドに動作するように設定され，定期的にデータを送受信していた，ということが推測される．この PC は，ウイルス対策ソフトはインストールされ，パターンファイルも常に最新になるよう設定されていることから既知のウイルス，スパイウェアではないと思われる [*6].

このことから，本稿における OS 検出には，2011 年当時には，Windows98 を User Agent に用いたプログラムが存在したことを考慮すると，実際とは異なる OS を User Agent に用いるプログラムが一定比率存在するため，推定精度を高めるためには定期的にログを精査して補正する必要があることがわかる．

また，何件か Windows XP と XP 以外の Windows OS 検出されている IP を数個ピックアップして調査したところ，同様なアクセスがあることを確認している．このことから，2014 年 4 月以降，本機能で Windows XP と検出さ

[*6] 一種の Adware であると推測されるが確認できていない．

```
(2280)133.x1.y1.z1(2014 年 0831-0907) の状況

    IP address 133.x1.y1.z1 (Http カウント=1069)
    Windows OS の状況
        未検出
    Windows Update の状況
        Update 実行 (未観測)
    Virus Scan ソフトのパターンファイル更新状況
        未検出
    利用ブラウザバージョン等の状況
        未検出
    Mac OS の状況
        未検出
    Mobile 機器の利用状況
        未検出
    Linux OS の状況
        未検出
    観測したブラウザの User-Agent の状況 (20 のみ表示)
        urlgrabber/3.1.0 yum/3.2.22
        WordPress/3.z.x; http:/([+/-][0-9A-Za-z]{5,}).(略)/
        WordPress/3.z.x; http:/([+/-][0-9A-Za-z]{5,}).(略)/en
        WordPress/3.z.x; http:/([+/-][0-9A-Za-z]{5,}).(略)/en/
        WordPress/3.z.x; http:/([+/-][0-9A-Za-z]{5,}).(略)
```

```
(2295)133.x2.y2.z3(2014 年 0831-0907) の状況

    IP address 133.x2.y2.z3 (Http カウント=83)
    Windows OS の状況
        未検出
    Windows Update の状況
        Update 実行 (未観測)
    Virus Scan ソフトのパターンファイル更新状況
        未検出
    利用ブラウザバージョン等の状況
        未検出
    Mac OS の状況
        未検出
    Mobile 機器の利用状況
        未検出
    Linux OS の状況
        未検出
    観測したブラウザの User-Agent の状況 (20 のみ表示)
        WordPress/3.5; http://(略)/
        WordPress/3.5; http://(略)
        urlgrabber/3.1.0 yum/3.2.22
```

図 8 WordPress 利用計算機情報の出力例

れた PC で他の Windows OS も併せて検出されているものは，バックグラウンドで不正なプログラムが通信を行っている可能性もあり，継続した監視・調査が必要であると思われる．

5.4 モバイル機器の利用状況把握例

神戸大学内の全学無線 LAN 以外の有線 LAN に，無線ルータあるいはブリッジを介して接続したと思われるモバイル機器の中で，Apple 社製 iPhone における各 OS バージョン検出数の推移を**図 7** に示す．ほとんどすべてのアクセスは NAT ルータ配下からのものであるため，検出数については，接続機器数の下界値であり，実際の接続機器数は異なる可能性が高いことに注意する必要がある．

図 7 から，以下のことが推測される．

- OS のバージョンアップが利用可能になってから, 短期間にユーザの半数程度がバージョンアップを実行する．
- 30%程度のユーザはバージョンアップを行わずに放置する．
- 10%程度のユーザは，新しいバージョンを利用できない古い機種を使い続けているか，かなり古いバージョンの OS バージョンをそのまま使い続けている．

今後，大学における情報化の対応においてモバイル機器への対応がさらに重要になってくることが予想される．図 7 に示すような状況を注視しながら今後の展開を行っていくことが重要であると思われる．また，モバイル機器におけるセキュリティが問題視されている．このような状況で，古いバージョンを使い続けることに対して対応を行う必要が出てくるものと思われるが，図 7 に示すような情報は，対策立案および実行状況の把握に際して重要な情報源となることが期待される．

5.5 アプリケーション利用状況把握への適用

Web ブラウザだけでなく，メールソフトウェア，オフィスソフトウェアなどのアプリケーションの中には，機能の一部に Web ブラウザの機能を持っていたり，アップデートの定期的なチェックなどの目的で HTTP 通信を行うものが多い．このようなアプリケーションが PC 上で利用された場合，本稿に述べた解析機能で検出・記録することができる．代表的なものとして以下のようなアプリケーションがあげられる．

- Microsoft Office (Windows 版)
- Thunderbird(メールソフトウェア)
- Dropbox

特に，セキュリティ上問題が発見されたアプリケーションが上記の条件に合致する場合は，本機能で検索することが可能である．

WordPress における Pingback 機能が DDOS 攻撃の踏み台になるという問題が発生した時 [5] に, 学内で WordPress がインストールされていると推測される IP を特定する時に本稿における機能を利用した．WordPress は，Update のチェックのために定期的に HTTP リクエストを発生させるている (2014 年時点) ため，本機能により検出可能である．**図 8** に検出した情報 (一部) を示す．

6. おわりに

本稿では，2012 年から取得している学外向け HTTP 通信のログ情報を用いて, 大学内で利用されている PC の利用状況を推定するために開発した解析機能について述べるとともに，Windows XP，モバイル機器, PC 上のアプリケーションの状況把握を行った事例について述べた．

本機能は，この他，インシデント対応時の対象 IP の状況把握などに利用しているが，迅速な調査に貢献している．今後は，プライバシーの問題を考慮しながら, セキュリティ上問題があると推測される PC の特定など情報セキュリティ維持への利用の他，ネットワーク/PC/モバイル機器の利用状況把握に適用していくとともに，ネットワーク上の通信記録の有効利用を促進するための情報セキュリティポリティーおよび利用指針の整備を進めていく予定である．

参考文献

[1] 情報処理推進機構: Windows XP のサポート終了に伴う注意喚起, 入手先 ⟨http://www.ipa.go.jp/security/ announce/winxp_eos.html⟩ (2014.05.15).
[2] Aruba Network: Data sheet: ArubaOS. 入手先 ⟨http://www.arubanetworks.com/pdf/products/DS_AOS.pdf⟩
[3] Gerald Combs, at al.: wireshark. 入手先 ⟨https://www.wireshark.org/⟩ (2014)
[4] The Apache Software Foundation: apache ログファイル. 入手先 ⟨http://httpd.apache.org/docs/2.2/en/logs.html⟩ (2014)
[5] 高橋睦美: 今度は WordPress が踏み台に、Pingback 機能を悪用し DDoS 攻撃. 入手先 ⟨http://www.atmarkit.co.jp/ait/articles/1403/13/news133.html⟩ (2014)