Vol.2016-IOT-35 No.15
Vol.2016-SPT-20 No.15
2016/9/24

ネットワーク接続記録収集によるネットワーク利用状況把握の試み

鳩野 逸生[1,a)]

概要：神戸大学では，2009 年 10 月のネットワーク導入後，ネットワークの利用状況の把握を目的として，2010 年 4 月から管理対象のエッジスイッチ (約 250 台) のすべてのポートに接続している機器の Mac アドレス, 割当 IP アドレスを一日 3 回記録している．来年度にネットワークの更新を控え，現ネットワークの運用・利用状況を接続データを用いて調査した結果を報告する．

1. はじめに

神戸大学では，2009 年 10 月のネットワーク更新 (KHAN2009)[1] 後，2010 年 4 月から管理対象の全エッジスイッチのすべてのポートを対象として, 1 日 3 回ポーリングして接続機器の情報を記録している．これは，次期ネットワーク更新においてエッジスイッチの配置および必要ポート数を決定する際に，ユーザからの要望とともに接続実績として用いるために実施しているものである．収集している情報は，接続機器の Mac アドレス, IP アドレス, 接続エッジスイッチ名，ポート番号である．

本稿では，来年度にネットワークの更新 (予定) を控え，Mac アドレスに含まれるベンダー情報を用いることによりどのような種類の機器がどの程度の期間接続されていたのかを中心とした調査を行ったので報告する．

2. 神戸大学ネットワークシステムの構成

2.1 ネットワーク構成

KHAN2009 の物理構成を図 **1** に示す．図 1 におけるコアスイッチは，Brocade 社 NetIron MLX-8, 各学部の入り口に設置した基幹スイッチには，Brocade 社 NetIron CES 2024F/2048FX, Juniper 社製 EX-4200-24F を利用しており，各学部のルーティングは各基幹スイッチで行う L3 構成となっている．また，無線コントローラには, Aruba 社製 Aruba 6000/3400, SSL-VPN 装置には, F5 社製 FirePass 4320，エッジスイッチには，H3C 社製 (現 HP 社) の L2 スイッチを採用している．

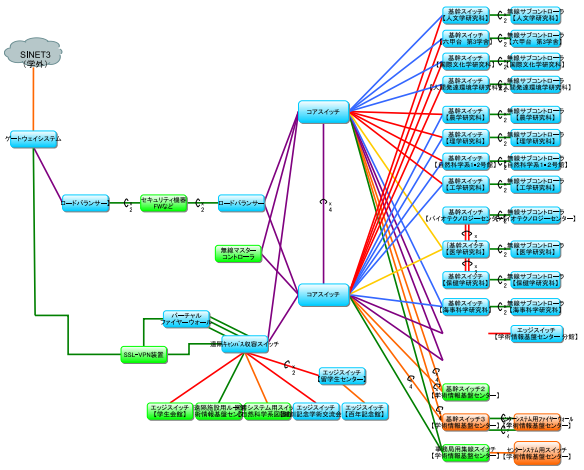


図 1 KHAN2009 の物理構成

3. 機器接続情報の収集

接続機器情報の収集は，一日 3 回 (11 時, 15 時，21 時) 以下に示す手続を，学部の入り口に設置された基幹スイッチ (L3 スイッチ) すべてで実施することにより収集している．

(1) 基幹スイッチ内の ARP テーブルを SNMP を用いて取得し，Mac アドレスと IP アドレスの対照表を作成する．

(2) 取得した ARP テーブルから管理アドレスの IP 領域にある機器のリストを取得する．

(3) 管理アドレス領域にある接続機器の Mac アドレス中で，エッジスイッチのベンダーコードを持たないものを除外する．

(4) 残った機器リストのすべてに対して，SNMP を用いて機器名を取得し，エッジスイッチの命名ルールに適合

[1] 神戸大学
Kobe Univ., 1-1 Rokko-dai, Nada, Kobe 657-8501, Japan
[a)] hatono@kobe-u.ac.jp

Vol.2016-IOT-35 No.15
Vol.2016-SPT-20 No.15
2016/9/24

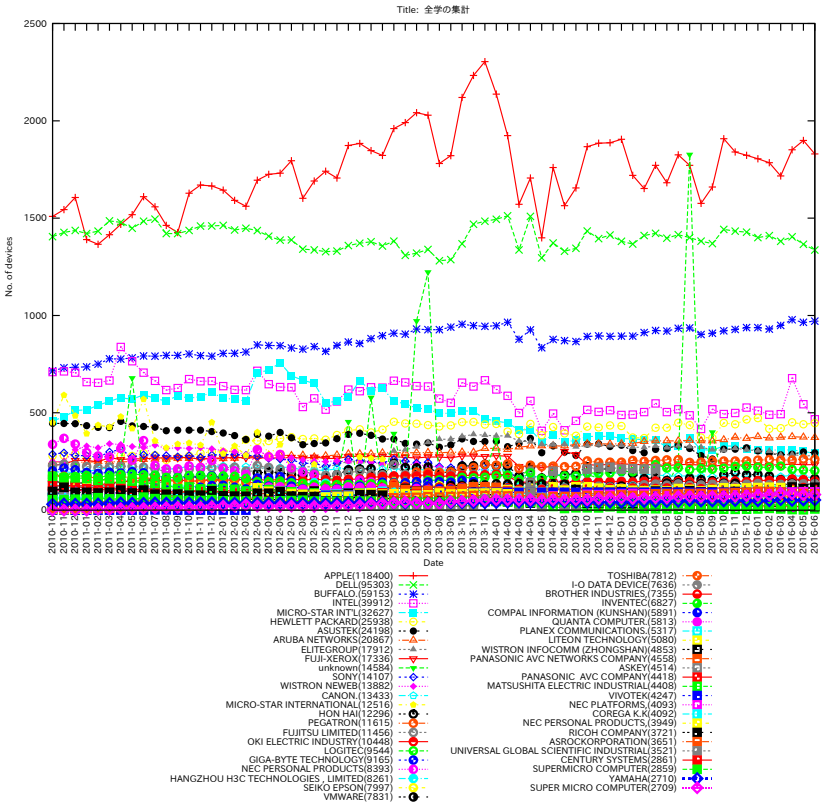


図 2　ベンダー情報毎の接続機器数の推移 (全学)

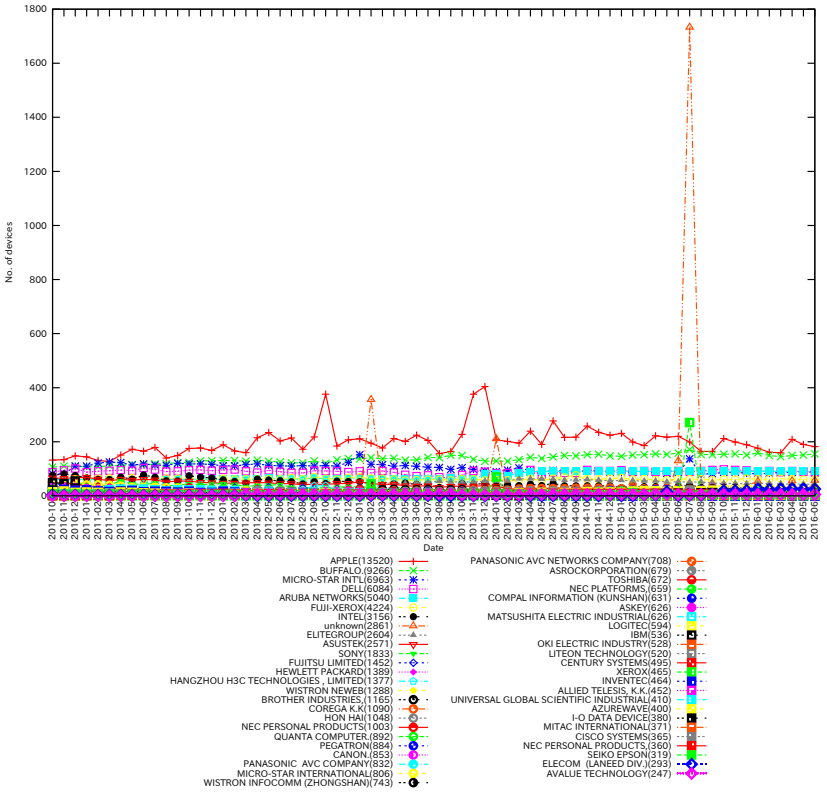


図 3　ベンダー情報毎の接続機器の推移 (学部 A)

しないものを除外する[*1].

(5) 検出されたエッジスイッチすべてに対して，各ポート毎に接続されている機器の Mac アドレスを SNMP を用いて取得する．

(6) 取得したエッジスイッチ/ポート番号/Mac アドレスの情報と基幹スイッチ内の ARP テーブルを照合し，割当 IP を付加して記録する．

本手続きにおいては，管理アドレスの空間から，エッジスイッチのベンダー情報および機器の命名規則を用いてエッジスイッチを探索しているため，エッジスイッチのリストを保持する必要はない．また，全学無線 LAN サービスに接続されている機器および情報基盤センターが設置している教育用端末 (約 1,300 台) は収集対象としておらず含まれていない．

収集された情報は，管理者用の Web サイトから，1 ヶ月単位で集計された情報が表示可能であるとともに，接続期間，IP, Mac アドレス, ベンダー名で検索可能なインタフェースを開発し, ユーザからのネットワーク障害申告時の状況把握にも利用している．

4. ベンダー情報による集計

図 2 に，2010 年 4 月から 2016 年 7 月までの 1 ヶ月毎に，エッジスイッチに接続された機器の Mac アドレスをベンダーで集計した図を示す．ただし，ベンダーは検出数の上位 50 位までをプロットしている．検出されているはずの機器は，神戸大学における教職員または研究室等に所属する学生が利用していると推測される．基本的に増減は機器の新規導入および廃棄であり, 短期間における大きな変動は例外的であると推測されるが，図 2 において, 機器の新規導入と廃棄では説明することが困難な極端な変動が数カ所見られる．以下に顕著なものを列挙する．

(1) **ベンダー不明**:

- 2011 年 5 月，2012 年 12 月，2013 年 6 月–7 月, 2015 年 7 月

(2) **ベンダー情報: Apple**

- 2013 年 12 月–2014 年 2 月

この中で，2015 年 7 月に発生した事象について詳細に調査した結果を以下に示す．

各学部ごとの集計をもとに調査したところ，ある学部 (以下，学部 A) において発生していたことが判明した．学部 A におけるベンダー情報の集計を**図 3** に示す．さらに詳細にエッジスイッチ毎の情報を調査したところ，2015 年 7 月 24 日に, 学部 A に設置されているあるエッジスイッチの 5 番ポートで 2774 個の Mac アドレスを 15 時に観測していることが判明した．当時ネットワーク障害の申告はなく，詳細は不明であるが，ベンダー情報不明な多数の Mac アドレスと共に，Xerrox のベンダー情報を持つものも多数観測していることら，Xerrox のプリンタ等を接続する際の HUB 等の故障か，ループが発生した可能性などが考えられる．

また，2013 年 12 月から翌年 2 月にかけて Apple のベンダー情報を持つ機器が大幅に減少している件に関しては，ある大規模理系学部が研究室等のネットワークを学部独自で導入したルータの配下に移動させたためであることが判明している[*2].

その他，図 2 において顕著なこととして，Buffalo など，ブロードバンドルータであると推測されるベンダーコードを持つ機器が常時，1,000 台以上接続されていることが分かる．これにより，有線ネットワーク上に検知される Mac アドレス数よりかなり多くの PC 等がネットワークに接続されていることが推測される．

5. 接続機器の入れ替え状況

図 4(1) および (2) に，全学における接続機器の総数および機器の入れ替えの状況を示す．図 4 において，“New Devices” および “Disappeared Devices” は，それぞれ，当該月に初めて検出した Mac アドレスの件数, および前月まで観測されていたが，該当月において観測されなかった Mac アドレスの件数を示している．図 4(1) において，2015 年 7 月頃に不自然な機器の増減が見られるが，これは前節で述べた障害により不正な Mac アドレスが観測されたためであると推測される．前節の例から，ベンダーが不

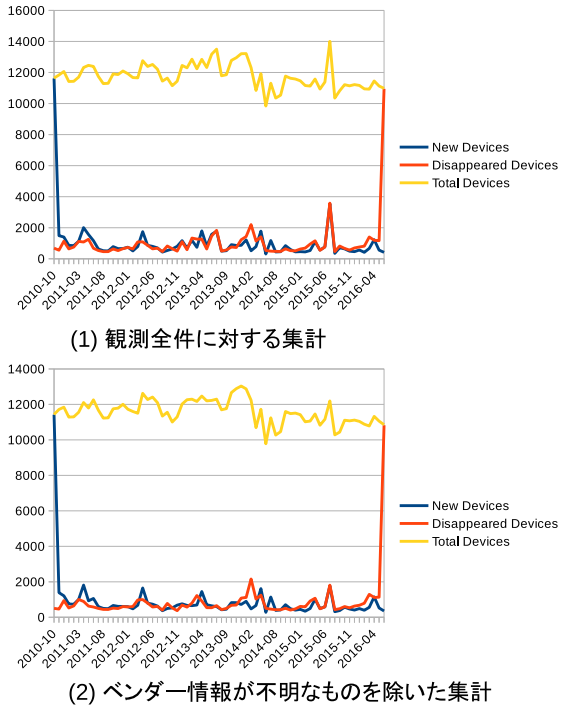


図 4 月毎の機器入れ替えの状況 (全学)

[*1] エッジスイッチ機器には， e- で始まる名前が付与されている．

[*2] 情報基盤センターに対して報告はなかった．

Vol.2016-IOT-35 No.15
Vol.2016-SPT-20 No.15
2016/9/24

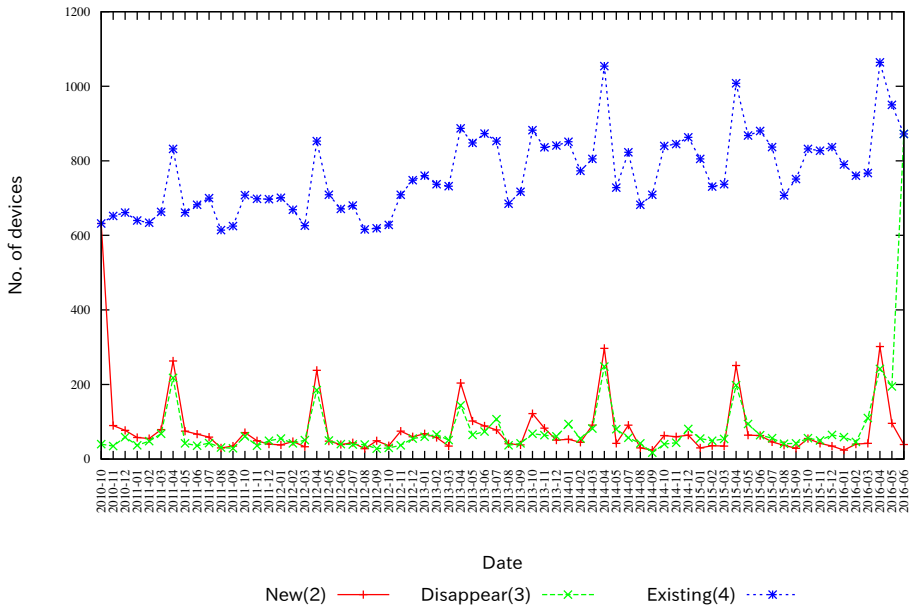


図 5　月毎の機器入れ替えの状況 (文系学部 A)

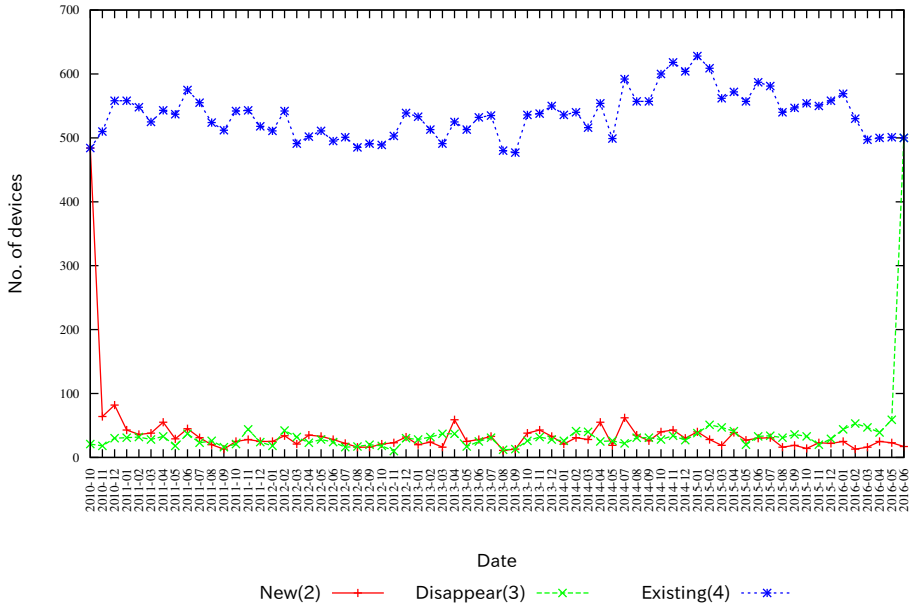
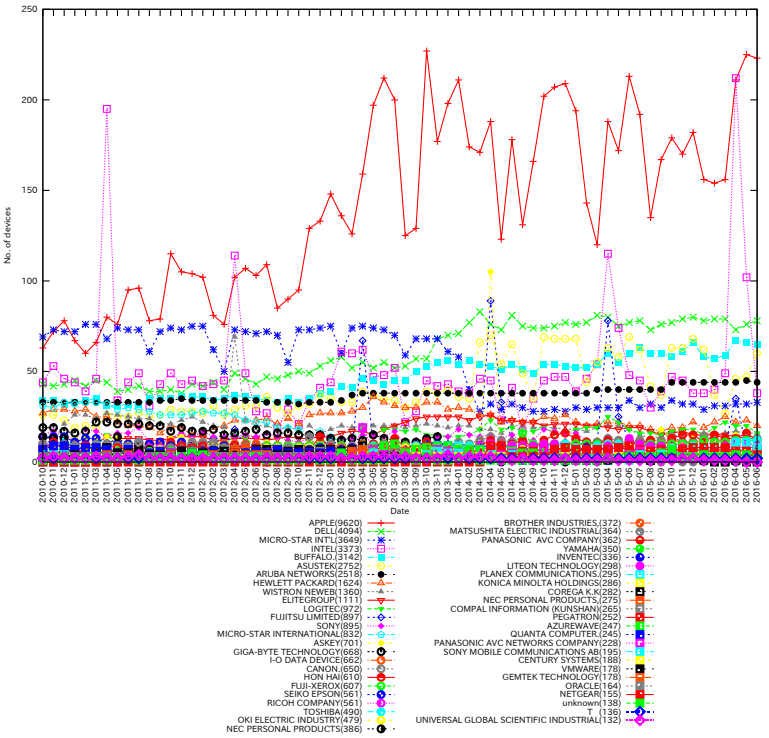
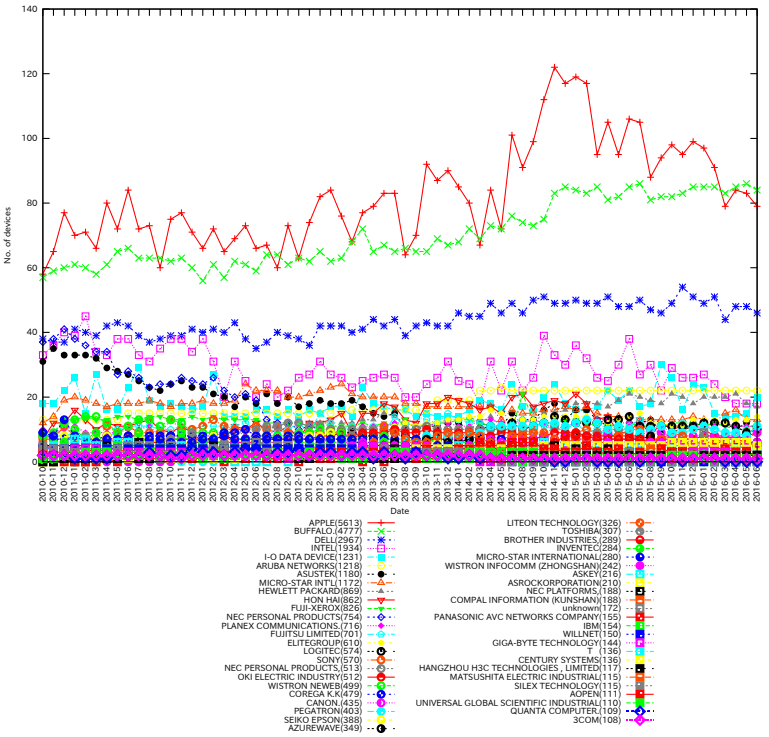


図 6　月毎の機器入れ替えの状況 (文系学部 B)

Vol.2016-IOT-35 No.15
Vol.2016-SPT-20 No.15
2016/9/24



(a) 文系学部 A



(b) 文系学部 B

図 7 文系学部 A および B におけるベンダー情報毎の接続数の推移

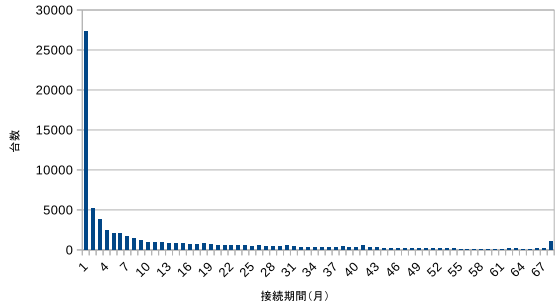


図 8　機器の観測観測期間分布 (補正無)

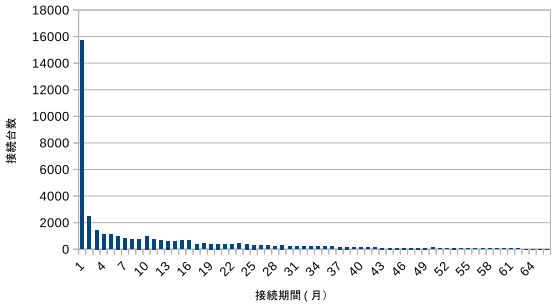


図 9　機器の観測観測期間分布 (補正後)

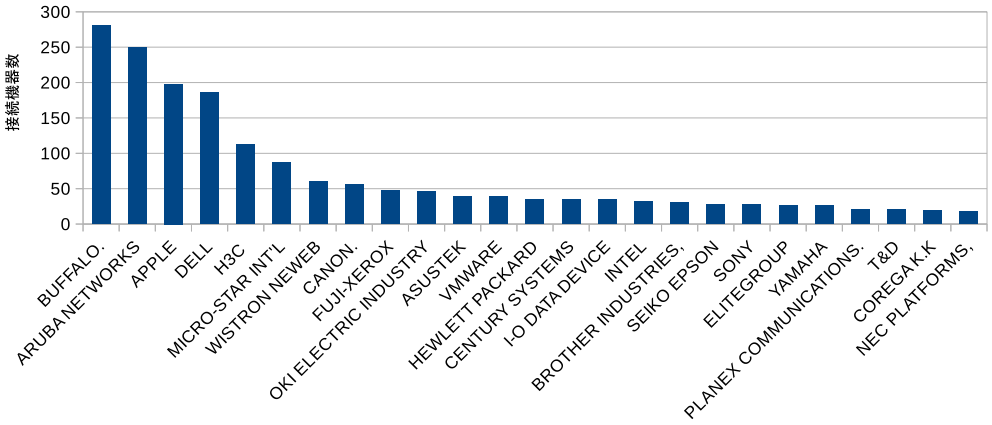


図 10　長期間接続されている機器

明な Mac アドレスは，何らかの機器の障害により発生した可能性が高く，接続機器の実数を反映していない可能性がある．図 4(2) に，ベンダーが不明な Mac アドレスを除いたグラフを示す．図 4(2) においては，図 4(1) に比べてやや 3–4 月においてやや多くの機器の入れ替えが行なわれている傾向がはっきりしていることが分かる．

神戸大学の文系学部 A, B における機器の入れ替え状況を**図 6**(1) および (2) に示す[*3]．文系学部 A においては，3 月から 4 月にかけて 200 台前後の機器の入れ替えが行なわれているのに対し，文系学部 B においては数十台程度であることが分かる．文系学部 B において入れ替え台数が少ないのは，ブロードバンドルータを介した PC 接続が多いためであることも考えられるため，**図 7** に，一ヶ月ごとの両学部における接続機器のベンダー情報毎の接続数を示す．図 7 から分かるように，新年度における入れ替え数が大きい文系学部 A の方がブロードバンドルータと推定されるベンダーコードを持つ機器 (Buffalo) が多く接続されている．以上のことから，実際には，文系学部 A では更に多くの機器の入れ替えが行なわれている可能性がある．ただし，文系学部 A においては，新年度付近で, INTEL のベンダーコードを持つ機器の接続数が一時的に極端に増加している．この現象は，何らかの障害によって発生している可能性もあるためより詳細な調査が必要である．

他学部毎のデータから，年度末から新学期にかけて多くの機器の入れ替えが行なわれており，入れ替え数は学部によりかなり異なっていることが判明している．しかし，本稿におけるデータ収集は，一日に 3 回しか行っていないため，ネットワークに接続されている時間が短時間の場合は検出されていない可能性が高い．接続台数の実数を推定するためには別途収集している HTTP の通信記録に含まれるソース IP などと組み合わせて補正を行う必要がある．

6. 機器接続期間

6.1 接続期間分布

2010 年 4 月から 2016 年 6 月にかけて観測された Mac アドレスで, 観測された接続月数の分布を**図 8** に示す．図 8 では，接続期間が短い機器が極端に多いことが分かる．これは，図 8 において集計を開始した 2010 年 4 月時点で接続されていた機器は,「接続一ヶ月目」として計上されているためであると思われる．これは，2010 年 4 月以前にどの程度の期間接続されていたかに関する情報がないためである．また，最終期間に接続されていた機器も「接続一ヶ月目」として計上されているが，期間以降も継続して接続される可能性が高い．さらに，対象データには，障害によって発生したと推測されるベンダーが特定できないものも数多く含まれている．従って，図 8 において，接続期間が短

*3　あくまでも集計対象の部局内での観測であり，他部局への移動は考慮していない．

い機器数は現実とかなり差があることが予想される．

より実数に近い分布を得るため，以下の条件を満たす満たすデータを全データから抽出して集計したものを図 **9** に示す．

データ抽出条件

- 対象期間の最初と最後の期間に観測されていない．すなわち，対象期間内に機器が導入されかつ廃棄された可能性が高い機器のみを対象とした．
- ベンダー情報が特定できない Mac アドレスをもつものは，障害によるものである可能性が高いため除外した．

図 9 において，依然としてかなり多くの機器が ごく短期間だけネットワークに接続されている状況が見て取れる．どのような状況でこのような接続が行なわれているかに関しては, 障害によって発生している可能性やセキュリティ上の問題がある可能性もあるため，今後調査する必要がある．

6.2 長期間接続されている機器

図 **10** に，対象期間中 60 ヶ月以上継続して接続されていると推測される機器 (60 期間で観測された機器) のベンダー情報毎の分布を示す．この中で，Aruba Networks および H3C は，基幹ネットワーク機器であり，考慮から除くと，家庭用のブロードバンドルータやプリンタであると推測されるベンダー情報をもつ機器が長期間接続されている傾向があることが見て取れる．長期間接続された家庭用ブロードバンドルータは，障害が多くなる傾向があるのとネットワーク更新で基幹部分が高速化されても古い機器が速度上のネックになる可能性もあり，対策が必要である．

7. おわりに

本稿では，2010 年 4 月から現在に至るまで蓄積されている有線ネットワーク上に接続されている機器情報を用いることにより，ネットワークの利用状況を推定することを試みた．その結果，過去にネットワークの障害が発生していたことが判明した．さらに，各月毎の機器更新数の推移が各学部ごとにかなり傾向が異なる，ブロードバンドルータやプリンタなどが長期間同一の機器が接続されていることなどが判明した．

今後は，次期ネットワークの更新において，各学部からの要望調査と本稿で得られた結果を照合することにより各学部におけるネットワークの管理・運用状況を推定しながら，設計を進めていく予定である．また，神戸大学では，学内から学外への HTTP の通信記録を取得している [2]．HTTP 通信記録から得られる OS や利用ブラウザ等の情報と組み合わせることにより，詳細な利用状況推定を進めていく予定である．

参考文献

[1] 鳩野逸生，伴好宏，佐々木博史: 神戸大学におけるネットワークシステムの構築, 情報処理学会研究報告，Vol.2009-IOT-7 No 1, pp. 1–5 (2009)
[2] 鳩野逸生, HTTP 通信ログ解析による学内情報機器の利用状況推定, 第 7 回インターネットと運用技術シンポジウム (IOTS2014) 講演論文集 (2014).