Vol.2010-DPS-142 No.8
Vol.2010-CSEC-48 No.8
2010/3/4

接続機種に最適なネットワーク接続を可能とするインフラストラクチャの構築

仲倉 利浩† 遠峰 隆史† 杉浦一徳†

インターネットの普及により，ネットワークに接続可能な機器や機種が爆発的に増えてきている．これらの機器インターネットへの接続は，どの機種でもハードウエアに依存し，機種によっての差異はない．これらインターネットにつながる機器は，OSI 参照レイヤーのデータリンク層によって，メーカーや機種の特定が可能となっている．
本研究では，各ノードにつながっている機種の MAC アドレスに着目し，MAC アドレスから得られるメーカーや製造機種を特定し，機種に最適なネットワークを構築する．

Building Infrastructure to Enable Connectivity Models for Optimum Network Connection.

Toshihiro Nakakura† Takashi Tomine†
Kazunori Sugiura†

The number of Devices or models which can be controled by network are rapidly increasing because of spread of internet.
These Devices and models depend on them hardwears in all respect of conection to internet and make no difference between each models.By checking OSI underlayer, we can distinguish its maker and its model which is conected by network.
In this reserch, we are going to aim at MAC adresses which are conected by node, and we going to go specify Devices' maker and production models.

*† 慶應義塾大学大学院メディアデザイン研究科
Keio University Graduate School of Media Design and Graduate School

1. はじめに

インターネットの普及は，PC，ノートパソコン，携帯電話，ゲーム機器などといった，ネットワーク接続可能な機種の爆発的な増加を促した．また，無線 LAN の機器の低価格化や公共のアクセスポイントの拡大，広帯域化はミニノート PC，タッチパッド PC，スマートフォン，携帯ゲーム機などの新しいポータブル機器を普及させた．インターネットの接続出来る機器の普及と拡大は，ネットワーク設計における接続限界を予測させた．

スケーラビリティの拡大は，図 1-1 に示されるように，より利便性を追求した製品(テレビ，インターネットラジオ，防犯機種，携帯ゲーム機，スマートフォンなど)もインターネットにつながり，サーバーや機器同士連携してサービスを行うことを可能とした．しかし，このことは公共の場所や家庭内でのネットワークの制御がより難しくなってくることを示している．

また，公共の場所でのワイヤレスネットワーク接続環境は，アクセスポイントの数，接続性，通信速度が上がってきており，各アクセスポイントについても，さまざまな機種がつながり，様々なサービスが受けられるようになってきた．現在，これらの公共のアクセスポイントやイベント会場でのネットワークは，無線における暗号化の技術で管理されており，接続機種に関係なく一様にアクセスできるようになっている[1].

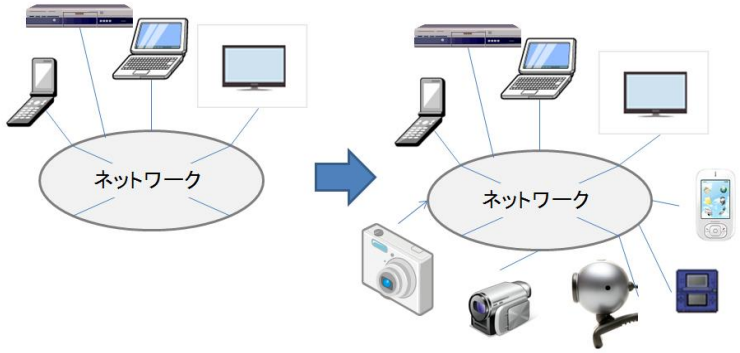

図 1-1 スケーラビリティの拡大による接続機種の増加

2. 研究目的

第 1 章で述べたネットワークに接続出来る機器の数の増加や機種の増加は，ネット

Vol.2010-DPS-142 No.8
Vol.2010-CSEC-48 No.8
2010/3/4

ワーク構築上や，管理上の問題となっている．特にイベントなどで設営されるネットワークは，つながる機種のメーカーや種類が多く，さらにワイヤレス接続で提供されることが多い．この為ネットワーク設営及び運営を行う上でのさらに難易度が高くなってきている．

このようなネットワークの最適化を行う上で，メーカーや機種を区別してネットワークの制御を行うことが出来る，Vender Driven なネットワークの構築が必要となってくる．

本研究は，メーカーごとに割り振られている MAC アドレスに着目し，メーカーや機種のより詳しい情報を抽出し，それに基づいたネットワーク制御を行うことを目指している．これを基とし，接続されている機種に沿ったサービスを提供することは，ユーザーにとって便利で快適なサービスが生まれる可能性を示している．

今回は，DHCP サーバーで蓄積されるログから，接続された機器の情報(メーカー/機種)を抽出し，ネットワーク制御に利用することが可能かどうか，実際のイベントで設営した，ネットワーク DHCP サーバーログを基に解析する．

上記の便利で快適サービスの具体例としては，ゲームイベント等で，ユーザーが操作すること無く機種ごとにその機種にあったサービスを提供したり，各社で操作性の異なるスマートフォンに情報を配信する場合，Vender 別の操作性にあった情報を提供したりするようなサービスである．

具体的な実現方法として， Vender 別に設定情報を提供し，別のサーバーに自動でアクセスさせることで，機種に最適なサービスを自動で提供出来るようになると考えている．

また，MAC アドレスの利用を考えている点については，MAC アドレスを用いて機種データの解析可能であれば，アプリケーションレイヤーまで解析することなく，OSI 参照モデルで示されるネットワークアーキテクチャのより下の層で機種を特定することが出来ることとなり，DHCP サーバーのプログラムの改変や，安価なハードウエアで，実現できる可能性が高くなくことになる．

MAC アドレスとは，ネットワーク製品の製造者が，MAC アドレスの管理を行なっている IEEE に割り当てと登録を受けており，Organizationally Unique Identifier(以下 OUI)と呼ばれる．OUI の下位の 24 ビットは各メーカーが独自に重複しないように割り当てている．メーカーが 1 つの OUI の割り当てを受けると，16,777,216 の製品に個別の MAC アドレスを機種に割り振ることができる．

この仕組みにより，原則として，MAC アドレスは世界中で唯一の番号となる．OUI の登録データは IEEE の Web ページにて確認することが出来る[2].

今回の研究では，イベントネットワークで取得したデータを利用して、そこで使用した DHCP サーバーのログデータを基に，実際のイベントネットワークに接続されている機種のメーカー及び機種の解析を進めていくものとする．

3. 研究の手法

3.1 MAC アドレスの取得方法

MAC アドレスの取得については、イベント会場に設置した DHPC サーバーのログから取得する方法を採用することとした．

ログデータは、準備期間中も含め、全てのデータが 1 つのファイルとなっている為，まずは準備期間と後始末の期間を除去し，開催日ごとに分けて解析を行うことにした．

必要なデータはログの中の ACK の送信でデータを抽出し行うものとする．理由としては，DHCP プロトコルのシーケンスの中で，クライアントに対し IP 設定情報を提供する為のメッセージとなっており，クライアントは ACK メッセージに内容に従いアドレスの設定を行うこととなっている為である[3].

ACK を抽出し重複した MAC アドレスを消去することにより，集計を行うものとする．重複が無くなったデータを元に IEEE のホームページでメーカー名を検索し，LIST に記載するものとする．上記の作業の後、MAC アドレス，IP アドレス，メーカー名，ホストネームの項目でテーブルを作成し，解析を行っていくものとする[4][5].

3.2 機種特定のアプローチ

今回は，DHCP ログでサーバー名が取得出来ることに着目し，接続機種を特定する検討を行う．具体的には，3.1 で作成したデーブルのサーバーネームに着目し，機種を特定出来るテキストデータより機種を特定し，MAC アドレスとの関連性があるかどうか，検討するものとする．

4. 実際のネットワーク

今回，私たちがネットワーク設営を行ったのは，開催期間が 4 日間，来場者数は延べ 2 万 5,000 人のイベントで，講演，シンポジュームを行うスペースと，展示スペースで構成されたイベントである．そのイベントで私たちは，講演や展示に必要なネットワークの構築以外に，イベントに訪れる来場者に対してインターネットへのアクセ

Vol.2010-DPS-142 No.8
Vol.2010-CSEC-48 No.8
2010/3/4

ス環境の提供を行った．

来場者に対しワイヤレスでネットワーク接続環境を提供することとした．また，IP アドレスはグローバルアドレスを準備し，DHCP サーバーを用いて割り当てた．

インターネットへの接続サービスは、ワイヤレスでこととした為，MAC アドレスから導き出されるメーカーは，製品を製造しているメーカーや販売しているメーカーではない可能性がある．また，一般にホームページで一般公開されている情報では，メーカー名や Vender 名のみで，それ以上の細かい情報を確認することは出来ない．2 章で説明したサービスを実現するために，機種によってもネットワークの制御を行いたいと考えているので，今回のネットワークで集めた情報を解析しての規則性や判別方法を見つけたいと考えている．

本論文はイベント 2 日目の DHCP ログデータを抽出し，メーカーや機種の特定が出来ないか解析を進めることとした．

4.1 MAC アドレスの割り当て状況

MAC アドレスの取得は，今回設置した DHPC サーバーのログファイルから取得することとした．今回使用した DHCP サーバーはデータベースによって管理される設定を行っており，一度接続が切られても同じアドレスが割り振られるようになっている．この状況の下で、ACK を抽出/整理し，MAC アドレスと IP アドレスの重複のとりまとめを行い，解析を進めていった．

結果、今回のイベント 2 日目の DHCP サーバーが割り当てた，IP アドレスは 1,030 個の IP アドレス割り当てを行っており，1,030 台の機種がネットワークに接続されたことが分かる．

4.2 ネットワークに接続されている機種のメーカー調査

5.1 で抽出した 1,030 台分 MAC アドレスより上位 24bit を抽出し，メーカー名を調査した結果，表 1 で示す通り、不明 1 社を含む 39 社の製品が，の設営したネットワークにアクセスしていることが分かった・

表 4-1　2 日目に接続されていたメーカー

ANSA Corporation	Liteon Technology Corporation
Apple, Inc	MICRO-STAR INT'L CO., LTD.
Arcadyan Technology Corporation	Motorola Mobile Devices
ASKEY COMPUTER CORP	Murata Manufacturing Co., Ltd.
ASUSTek COMPUTER INC.	Nintendo Co., Ltd.
AzureWave Technologies, Inc	Nokia Danmark A/S
Buffalo Inc.	PLANEX Communications INC
CADMUSCOMPUTER SYSTEMS	QCOM TECHNOLOGY INC.
Cameo Communications, INC.	Quanta Computer Inc
COMPAL INFORMATION (KUNSHAN) CO., LTD.	Quanta Microsystems, INC.
Dell Inc	Research In Motion
EyeFi, Inc	Samsung Electro-Mechanics Co., Ltd.
FOXCONN	SHARP CORPORATION
Gemtek Technology Co., Ltd.	Sony Computer Entertainment Inc.
Hewlett Packard	Sychip Inc.
High Tech Computer Corp	UniData Communication Systems, Inc.
Hon Hai Precision Ind.Co.,Ltd.	VIA Networking Technologies, Inc.
HTC Corporation	VMware, Inc.
IBM Corporation	Wistron Corp.
Intel Corporate	

なお，Apple Inc.と Apple Computer Inc.などは同一メーカーとして扱っている．

これにメーカー名の情報に接続台数を入れてグラフにすると，図 4-1 のようになり，設営したネットワークのその日の接続機器として，Apple Computer Inc.の製品が一般的な市場のシェアより多く，51%を締めていることが分かった．

Vol.2010-DPS-142 No.8
Vol.2010-CSEC-48 No.8
2010/3/4

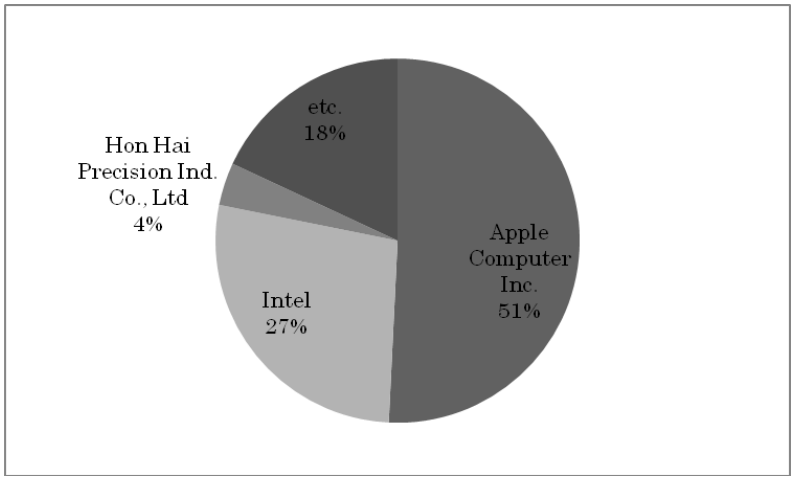

図 4-1 メーカー別の接続割合

また、解析結果より，Intel と Hon Hai Precison Ind. Co.,Ltd. の 2 社が，メーカーの上位に入ってきている．これは，この 2 社がノート PC 用に Wi-Fi のモジュールを生産しているからである．これにより，Apple 社以外のノート PC について、DHCP サーバーログより解析を進めることを難しくしている．

4.3 DHCP ログに含まれるサーバー名から機種を特定するアプローチ

DHCP ログからは，サーバー名の取得が可能となっている．取得したサーバー名より，機種接続されている機種を類推することが可能であるが，サーバー名はユーザーによって変更可能な為，確実に機種の特定を行える物ではない[6].

4.3.1 Apple Inc.及び Apple Computer Inc.機種特定

Apple, Inc 及び Apple Computer Inc.の MAC アドレスを抽出し，ホストネームを調査する．検証内容及び結果は，(1)～(3)に記す．

(1)iPod Touch

作成したテーブルを MAC アドレス上位 24bit で順番に並べ，ホストネームの項目から iPod Touch と思われる記載が多い部分を上位 24bit が共通な物単位で抽出する．抽出したデーブルを下位 24bit で並び換えを行い，解析を行って行った．

なお，下位 24bit 部分とホストネームの部分は実際には情報が入っているが．

表 4-2　OUI が 00:1d:4f を抽出し iPod Touch を示した

上位24bit	下位24bit	製造メーカー	IPアドレス	ホストネーム
00:1d:4f	95:c5:d4	Apple Computer Inc.		via133.22.32.1
00:1d:4f	96:c1:c4	Apple Computer Inc.		(Fanfans-itouch)via133.22.32.1
00:1d:4f	9c:4a:80	Apple Computer Inc.		(kameiPod)via133.22.32.1
00:1d:4f	9e:61:68	Apple Computer Inc.		(iPod)via133.22.32.1
00:1d:4f	a3:fb:11	Apple Computer Inc.		(Noriz-touch)via133.22.32.1
00:1d:4f	af:45:01	Apple Computer Inc.		(iPod)via133.22.32.1
00:1d:4f	b6:b8:61	Apple Computer Inc.		(iPod-touch-7)via133.22.32.1
00:1d:4f	c3:5d:19	Apple Computer Inc.		(tyndall)via133.22.32.1
00:1d:4f	d4:da:cd	Apple Computer Inc.		(shinjis-ipod-2)via133.22.32.1
00:1d:4f	d8:81:ed	Apple Computer Inc.		(Kanasai)via133.22.32.1

はホストネームからiPod touchと類推出来たMACアドレス
それ以外は、ホスト名では判別不可能だったMACアドレス

網掛けはホストネームより iPod Touch と類推された物を示している．また、iPod Touch と類推するに当たり，判断材料とした Word は「touch」，「ipod」である．これは，iPhone のホスト名の初期値が「○○の iPod」(○○はユーザー名)となっている為である．また，touch は製品名であり，複数の Apple 製品を使用しているユーザーがホストネームを分ける為に使う可能性がある．図 5-3 より iPod Touch と類推された項目に連続性があり，その他の機種が混在していない．このことから，00:1d:4f 全ての MAC アドレスが iPod touch に割り振られていると類推することとした．

(2)iPhone

同様に iPhone についても同様の手順で処理を行い，テーブルを作成した．

Vol.2010-DPS-142 No.8
Vol.2010-CSEC-48 No.8
2010/3/4

表 4-3. OUI が f8:1e:df を抽出し iPhone を示した

上位24bit	下位24bit	製造メーカー	IPアドレス	ホストネーム
f8:1e:df	07:d4:2d	Apple Computer Inc.		(Daniels-iPhone)via133.22.32.1
f8:1e:df	26:8b:14	Apple Computer Inc.		(uri)via133.22.32.1
f8:1e:df	2c:b6:06	Apple Computer Inc.		via133.22.51.1
f8:1e:df	32:43:12	Apple Computer Inc.		(iPhone)via133.22.32.1
f8:1e:df	32:e0:ad	Apple Computer Inc.		(takibi-iPhone)via133.22.32.1
f8:1e:df	45:fe:e9	Apple Computer Inc.		(Maddots-iPhone)via133.22.32.1
f8:1e:df	4e:ef:5d	Apple Computer Inc.		(mPhone)via133.22.32.1
f8:1e:df	70:b8:56	Apple Computer Inc.		(iPhone)via133.22.32.1

はホストネームからiPod touchと類推出来たMACアドレス
それ以外は、ホスト名では判別不可能だったMACアドレス

網掛けはホストネームより iPhone と類推された物を示している. iPhone と類推するに当たり，判断材料とした Word は「iphone」，「phone」である．これは，iPhone のホスト名の初期値が「○○の iPhone」(○○はユーザー名)である為．また，phone を判断材料にしたのは，複数の Apple 製品を利用しているユーザーの場合，機器の種類である Phone を利用する可能性があり，Apple 社が iPhone 以外に電話を企画/製造していない為である.

図 5- 3 より iPhone と類推された項目に連続性があり, その他の機種が混在していない．このことから，f8:1e:df の全ての MAC アドレスが iPhone に割り振られていることが類推される.

(3)複数の機種が混在している OUI についての解析

Apple Computer Inc.の OUI の中で，00:25:00 はホストネームから複数の機種が混在している. この部分の解析を行っていく上で, OUI 情報のみでは判断がつかないので, その下の 8bit も含めて規則性を調査していくこととする.

表 4-4　OUI が 00:25:00 で抽出し機種別表示を行った

上位24bit	中位8bit	下位16bit	製造メーカー	IPアドレス	ホストネーム
00:25:00	13:		Apple Computer Inc.		
00:25:00	15:		Apple Computer Inc.		
00:25:00	1d:		Apple Computer Inc.		
00:25:00	33:		Apple Computer Inc.		
00:25:00	3e:		Apple Computer Inc.		
00:25:00	3e:		Apple Computer Inc.		
00:25:00	3f:		Apple Computer Inc.		
00:25:00	40:		Apple Computer Inc.		
00:25:00	41:		Apple Computer Inc.		
00:25:00	41:		Apple Computer Inc.		
00:25:00	49:		Apple Computer Inc.		
00:25:00	49:		Apple Computer Inc.		
00:25:00	4a:		Apple Computer Inc.		
00:25:00	4a:		Apple Computer Inc.		
00:25:00	4c:		Apple Computer Inc.		
00:25:00	4c:		Apple Computer Inc.		
00:25:00	4c:		Apple Computer Inc.		
00:25:00	4c:		Apple Computer Inc.		
00:25:00	4d:		Apple Computer Inc.		
00:25:00	73:		Apple Computer Inc.		
00:25:00	7d:		Apple Computer Inc.		
00:25:00	86:		Apple Computer Inc.		
00:25:00	92:		Apple Computer Inc.		
00:25:00	f9:		Apple Computer Inc.		
00:25:00	f9:		Apple Computer Inc.		
00:25:00	fa:		Apple Computer Inc.		

iPod touch
Mac Book Pro
iPhone
Mac Book Air

網掛けはホストネームより iPod，iPhone，Mac Book Pro，Mac Book Air と類推されている．iPod，iPhone は(1)，(2)と同様の Key Word で類推した．Mac Book Pro と類推するに当たり, 判断材料とした Word は「BookPro」,「MBP」である. これは, MacBookPro のホスト名の初期値が「○○の MacBookPro」(○○はユーザー名)となっている為である．また，MBP は MacBookPro の短縮系であり，これも判断材料として使えると思われる.

また，Mac Book Air については「Air」を Key Word で類推した． これは，Air が製品

Vol.2010-DPS-142 No.8
Vol.2010-CSEC-48 No.8
2010/3/4

名であることより，利用することとした．

図 4-4 よりと類推した各機種について MAC アドレスが連続的に割り振られている．

(4) Apple Computer Inc.の機種での接続集計

この結果をもとに，上位 24bit+下位 8bit で上記の内容で判別出来るものがあれば，その MAC アドレスは同一のカテゴリーに割り振ることとし，Apple Computer Inc.の接続を解析していくこととした．

この為，上位 24bit 単独，上位 24bit+下位 8bit で類推出来ない物は不明として接続の機種の構成比率を求めることとした．

具体的には，MAC アドレスで Apple Computer Inc.の製品と判別出来る物を抽出し，MAC アドレス上位 24bit とその次の 8bit で並び換えを行い，前述の方法に従って機種の特定を行う．次に，機種が特定された MAC アドレスと上位 24bit+下位 8bit が一致する物を同一機種と類推し機器の特定を行い，数を集計しその割合を集計する．

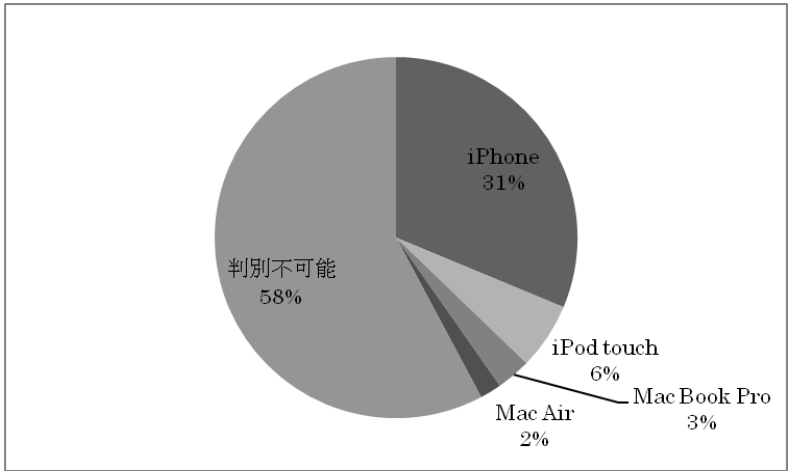

図 4-5 Apple 社製品の機種別情報

4.3.2 その他特定可能な機種

HDCP サーバーログの解析結果より，Apple Computer Inc.以外で機種の特定が出来そうな物についての解析結果を記載する．

(1) Research In Motion 社

今回のイベントで設営したネットワークにつながった Research In Motion 社の製品は 10 台で，ホストネームには BLACKBERRY の Key Word が含まれており，全てが BLACKBERRY 端末であると類推される．

表 4-6 OUI が 00:1d:4f で抽出した場合のホストネーム

上位24bit	下位24bit	製造メーカー	IPアドレス	ホストネーム
00:25:57	[redacted]	Research In Motion	[redacted]	(BLACKBERRY [redacted]
00:25:57		Research In Motion		(BLACKBERRY
00:25:57		Research In Motion		(BLACKBERRY
00:25:57		Research In Motion		(BLACKBERRY
00:25:57		Research In Motion		(BLACKBERRY
00:1 c:cc		Research In Motion		(BLACKBERRY
00:23:7a		Research In Motion		(BLACKBERRY
00:21:06		Research In Motion		(BLACKBERRY
00:24:9f		Research In Motion		(BLACKBERRY
00:24:9f		Research In Motion		(BLACKBERRY

(2) Nintendo Co., Ltd.社

ゲームメーカーの Nintendo Co., Ltd.の製品は 2 台が接続しており，図 2 台とも DS であったと類推される．

表 4-7　OUI が 00:1d:4f で抽出した Nintendo Co., Ltd.のホストネーム

上位24bit	下位24bit	製造メーカー	IPアドレス	ホストネーム
00:16:56	[redacted]	Nintendo Co., Ltd.	[redacted]	(NintendoDS)
00:22:aa		Nintendo Co., Ltd.		(NintendoDS)

5. 結論

MAC アドレス単体では，機種の製造メーカー又は NIC の製造メーカー，Vender 名以外の内容を判別することは出来なかったが，その他の情報と組み合わせることで，機種を特定出来る可能性があることが分かった．このことにより，DHCP サーバーの機能として，MAC アドレスを元に，ゲートウェイの設定を変更し，2 章で提案したような公共の空間内で Vender に依存サービスが提供出来る．

Vol.2010-DPS-142 No.8
Vol.2010-CSEC-48 No.8
2010/3/4

また，今回利用したのは，ACK データの MAC アドレス，IP アドレス，ホストネームであったが，ログの中にはその他のデータや，時系列ごとの手順なども残されている為，この部分からの解析も検討する必要がある．

但し，ある種の機種の MAC アドレスはユーザーが書き換え可能であるため，また，ホストネームに関しても同様に，ユーザーが書き換えや偽ることが可能な為，単独でネットワーク環境設定に利用した場合，ユーザーの利便性を著しく損なう可能性が出てくる．

6. おわりに

本論文では，4 日間のイベントの内の 1 日のみで解析を行ったが，その他の開催日についても解析を進め，機種特定のデータを蓄積して行く必要がある．また，準備期間については，開催日にとは違う機種がつながっている可能性があるので，分析を進めて行こうと考えている．

今後，第 4 章で取り上げた以外の製品についても判別方法を特定出来るように，解析を進め，本研究の最終目標である，イベント会場でのサービス提供に使用したサービス実現していきたい．

ただし，公共の場所のネットワークでの機種判別を行う方法を検討すると言うことは，機種固有の脆弱性を突いた攻撃を可能とすることもある為，この点も考慮に入れ，研究を進めて行く必要がある．

参考文献

[1]Microsoft Windows Embedded Standard
http://msdn.microsoft.com/ja-jp/library/bb499400(WinEmbedded.51).aspx
[2]IEEE OUI 検索ホームページ http://standards.ieee.org/regauth/oui/index.shtml
[3]ネットワークエンジニアとして　http://www.infraexpert.com/study/dhcp.htm
[4]DHCP org home page http://www.dhcp.org/
[5]RFC2131　ftp://ftp.rfc-editor.org/in-notes/rfc2131.txt
[6]山崎はるかの HP(MAC do: MAC アドレス書き換えソフト)　http://www.nda.co.jp/memo/macdo/