

推薦論文

## DLNA Probe : DLNA デバイスの操作履歴取得システム

猿 渡 俊 介<sup>†1</sup> ヨハン イェルム<sup>†2</sup>  
小 田 稔 周<sup>†2</sup> 森 川 博 之<sup>†1</sup>

さまざまな家庭内でのユーザの行動情報を収集することで、新しいサービスや商品の研究開発に役立てることができる。行動情報の収集に向けては、実際の家庭内でのユーザの行動情報を簡単に取得するための実験ツールが必要となる。本論文ではすでに家庭内に展開されつつある DLNA デバイスの存在に着目し、DLNA デバイスの操作履歴を取得するシステム「DLNA Probe」の設計、実装、評価について述べる。DLNA Probe では、ARP スプーフィングを用いて DLNA デバイス間の通信を DLNA Probe 経由になるようにリダイレクトすることでモニタリングを実現する。これにより、既存の DLNA の枠組みを壊すことなく、DLNA デバイスの操作履歴を収集することができる。

### DLNA Probe: A System for Logging Operation History of DLNA Devices

SHUNSUKE SARUWATARI,<sup>†1</sup> JOHAN HJELM,<sup>†2</sup>  
TOSHIKANE ODA<sup>†2</sup> and HIROYUKI MORIKAWA<sup>†1</sup>

We can extract user activity data, such as when and how the users enjoy multimedia contents, from operation history of DLNA devices. The activity data are useful for ethnography, context-aware recommendation services, and so on. In this paper, we show DLNA Probe, a system for logging operation history from DLNA devices by monitoring communication among the DLNA devices. The DLNA Probe combines SSDP and ARP spoofing, and the combination redirects traffic among DLNA devices toward DLNA Probe. The redirection enables DLNA Probe to log operation history of DLNA devices without changing any specification of DLNA.

### 1. はじめに

家庭内におけるさまざまな情報を取得してコンテキスト情報を抽出することで、ユーザにとって便利なサービスを提供することができる。これに向け、ユーザの行動情報を取得したり利用したりするための研究開発が活発化している<sup>1)-10)</sup>。また、ECHONET<sup>11)</sup> や OSGi (Open Services Gateway initiative)<sup>12)</sup> でも、家庭内の機器から操作履歴を取得するための規格が制定されている。しかしながら、ECHONET や OSGi への対応はエアコンなどの一部の機器に限られていることや、新築住宅などの一部の環境でしか活用できる環境が整っていないことなど、既築住宅への展開は課題が残っている。

筆者らは、さまざまな家庭でのユーザの行動情報を収集することで、新たな知見の獲得や新しいサービス・商品の研究開発に貢献することを目指している。これに向けては、実際にユーザが生活している環境でユーザの行動情報を簡単に収集可能な実験ツールの提供が鍵となる。このような観点から、本研究では、すでに一般家庭にも展開されつつある DLNA (Digital Living Network Alliance)<sup>13)</sup> の存在に着目し、DLNA デバイスの操作履歴を取得する。DLNA デバイスの操作履歴を抽出することで、ユーザがいつ DLNA デバイスを起動し、どのようなタイミングでどのようなコンテンツを閲覧したかなどが分かる。このような DLNA デバイスの操作履歴を取得することができれば、コンテンツ推薦サービスなど行動情報の利活用への発展も期待できる。

本論文では、DLNA デバイスの操作履歴を取得するシステム「DLNA Probe」の設計、実装、評価を示す。DLNA Probe では、ARP (Address Resolution Protocol) スプーフィングによって DLNA デバイス間の通信が DLNA Probe を経由するようにリダイレクトすることでモニタリングを実現する。本論文の貢献は以下の 3 点である。1 つ目は、SSDP (Simple Service Discovery Protocol)<sup>14)</sup> と ARP スプーフィングを組み合わせることで、既存の DLNA の枠組みを壊すことなく、DLNA デバイス間の通信のみをモニタリングすることができることを示した点である。2 つ目は、DLNA デバイス間の通信のみをモニタリングするための ARP スプーフィングの要件を明らかにした点である。3 つ目は、SSDP と

<sup>†1</sup> 東京大学先端科学技術研究センター  
RCAST, The University of Tokyo

<sup>†2</sup> 日本エリクソン株式会社  
Ericsson Research Japan

本論文の内容は 2010 年 1 月のモバイルコンピューティングとユビキタス通信研究会にて報告され、同研究会主催により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である。

ARP スプーフィングを用いた DLNA デバイスの操作履歴取得手法を DLNA Probe として実装し、評価した点である。評価では、DLNA Probe を用いた場合に、DLNA のコンテンツ保護技術である DTCP-IP (Digital Transmission Content Protection over Internet Protocol)<sup>15)</sup> の要求遅延 7ms を満たせるかどうかを明らかにするために遅延の計測を、配送可能なトラフィック量を明らかにするためにスループットの計測を行った。

本論文の構成は以下のとおりである。まず、2 章で、既存のユビキタスコンピューティングやユーザモデリングの分野で行われているユーザの行動情報の取得や利活用の研究開発を概観し、本研究で DLNA デバイスの操作履歴の取得に着目した理由を明らかにする。次に 3 章で、本論文で提案する DLNA デバイスから操作履歴を取得するための DLNA Probe の全体像と各機構の詳細について述べる。4 章で DLNA Probe の実機評価を示し、最後に 5 章でまとめとする。

## 2. 関連研究

ユーザが実際に生活している際の行動情報を収集することで、新たな知見の獲得や新しいサービス・商品の研究開発に貢献できる。たとえば、収集した行動情報を、家電やネットワーク機器の省電力性を実現する研究<sup>16),17)</sup> の評価データとして利用することや、異常検出のアルゴリズムの研究<sup>18)</sup> に役立てることができる。

行動情報の収集に向けては、今まさに展開されつつある情報家電の規格に行動情報を収集するための仕組みを導入することが理想的である。しかしながら、行動情報を利用して実現できるサービスや行動情報を収集すること自体の有効性を明確にしてからでなければ規格化することは困難である。これに向けては、ユーザが生活する家庭内に簡単に導入可能な行動情報を取得するための実験ツールが求められる。

### 2.1 行動情報取得技術

現在、ユビキタスコンピューティングやユーザモデリングの研究コミュニティを中心に、実空間でのユーザの行動情報を蓄積することを目指して多くの研究がなされている<sup>1)-10)</sup>。実空間上で取得された情報はコンテキストウェアサービス、推薦サービス、エスノグラフィなどさまざまな分野へ応用できる。たとえば、MIT の Place Lab では、百以上のセンサを生活空間を模した環境に埋め込み、ユーザが実験的にその環境で生活した際の情報を取得して公開している<sup>2)</sup>。Place Lab で取得された情報は、家庭内の電力消費を削減するコンテキストウェアサービスの研究などで利用されている<sup>16)</sup>。Zancanaro らの研究<sup>1)</sup> では、美術館で得たユーザの移動履歴を用いてユーザの行動パターンを教師なし学習で分類した

結果、エスノグラフィで得られた分類と同様の分類が可能であることが示されている。

ECHONET<sup>11)</sup> を用いることで、家庭内のユーザの行動情報を ECHONET 対応デバイスを介して詳細に取得することができる。ECHONET は、人体検知センサや温度センサなどの家庭内の設備とともに、エアコンや空気清浄機などの白物家電をネットワーク化するための規格である。ECHONET のイベント通知機能を利用することで、設備系のセンサや白物家電から情報を取得することができる。ECHONET と、Java モジュールの動的追加と実行を管理するための仕様である OSGi<sup>12)</sup> とを組み合わせると、機器の動作履歴や故障履歴を蓄積することも検討されている。ECHONET 対応機器はすでに 1,000 万台規模で展開されており、一般家庭にも設置され始めている<sup>19)</sup>。しかしながら、設置されている ECHONET 対応機器はエアコンなど一部の機器に限られており、新築のマンションで一括採用されることはあっても既築住宅に展開されている例は少ない。

### 2.2 DLNA デバイスの操作履歴の取得

行動情報取得技術の家庭内への展開という課題に対し、筆者らはすでに実際の家庭内に展開されつつある DLNA<sup>13)</sup> デバイスの存在に着目する。DLNA は家庭内でのメディア機器、PC、モバイル機器などの娯楽家電の相互接続を実現するための業界標準である。すでに多くの企業がテレビ、ブルーレイディスクレコーダ、デジカメなどの DLNA デバイスを販売しており、徐々に一般家庭内にも普及し始めている。

また、DLNA を拡張する試みも積極的に進められており<sup>20)-33)</sup>、ユーザが動画、音声、静止画などのマルチメディアコンテンツにアクセスする際の中心となる技術になることが予想される。現時点でも、YouTube の動画を DLNA デバイスで閲覧可能とする製品、DLNA と SNS を連携させて友だちや家族とコンテンツを共有するサービス<sup>20)</sup>、サードパーティにホームネットワーク内のコンテンツを提供するための技術<sup>21)</sup>、IPTV や IMS と融合するための技術<sup>22),23)</sup>、モバイルデバイスや外部のホームネットワークからインターネットを介して DLNA デバイスにアクセスするための技術<sup>24)-33)</sup> などの研究開発が進められている。DLNA デバイスの操作履歴を簡単に取得可能なツールを提供することで、DLNA を拡張するこれらの研究開発に対して、デバッグや実際に開発したサービスがどのように使われているかの分析などの点で貢献できると考えている。

また、DLNA の操作履歴は、新しいサービスや商品の研究開発に役立てることができると考えている。新しいサービスの例として、コンテキスト情報を利用した推薦サービスがあげられる<sup>34),35)</sup>。DLNA デバイスの操作履歴を取得した結果としてユーザが夜間に音楽を聴きながらショートコンテンツを楽しむ「ながらユーザ」であることが抽出できた場合、

ながら作業でも楽しむことができるようなショートコンテンツをお勧めする推薦サービスを提供することができる。

エスノグラフィ的な観点では、DLNA デバイスをどのようにユーザが利用するかが観察できれば新商品の開発のヒントを得ることも可能であろう。たとえば、ビジネス・エスノグラフィでは、ユーザの行動がどのような動機のもとで行われているかといった、深いレベルでのユーザの定性的な側面を理解するために、例外的ユーザを対象にフィールドワークを実施する<sup>36)</sup>。さまざまな家庭の DLNA デバイスの操作履歴を集めることで、毎朝必ず 1 時間コンテンツを閲覧するユーザや、DLNA のヘビーユーザなどの例外的ユーザを発見することに役立てることができる。

DLNA デバイスの操作履歴を取得する方法として、DLNA デバイス自身が直接操作情報を通知する手法が考えられる。DLNA の基盤となっている UPnP<sup>37)</sup> はイベントを通知する GENA<sup>38)</sup> と呼ばれる仕組みを持っているため、GENA でユーザの操作情報を通知すれば操作履歴を取得することができる。たとえば、DLNA の DMR (Digital Media Renderer) では複数の DMC (Digital Media Controller) による操作の同期のために GENA を用いて操作履歴を通知する仕組みを提供している。

しかしながら、現状の DLNA では DMR における再生イベントなどのごく一部のイベントしか通知しない。たとえば、DMP (Digital Media Player) は DMR と同様に動画を再生する機能を有しているが、DMC から制御されることを前提としていないため、イベントの通知は行わない。

### 2.3 通信のモニタリングによる操作履歴の取得

現在の DLNA の枠組みを拡張することなく操作履歴を取得する方法として、DLNA デバイス間の通信をモニタリングする手法が考えられる。モニタリングするには、既存の DLNA サービスに影響を与えないことが求められる。たとえば、DLNA の著作権保護技術である DTCP-IP<sup>15)</sup> では、DLNA デバイス間の遅延が 7ms 以下の場合のみにコンテンツの配送を許可するため、モニタリングによって遅延が 7ms を超えることは避けなければならない。

ホームネットワークがすべてリピータハブを用いて構築されていればイーサネットのプロミスキャスモードを用いてすべてのトラフィックをモニタリングすることができる。しかしながら、現在の家庭内ではリピータハブはほとんど用いられておらず、スイッチングハブや無線 LAN が用いられているため、イーサネットのプロミスキャスモードを用いたとしても通信をモニタリングできるとは限らない。

DLNA デバイスの通信をモニタリングするためにミラーリングポートを備えたネットワーク機器を導入する方法も考えられる。ミラーリングポートは、スイッチや無線 LAN アクセスポイントを経由するすべてのパケットの複製を出力するポートであり、IDS (Intruder Detection System) などに利用されている。出力されたすべてのパケットを解析することで、DLNA デバイスの通信をモニタリングすることができる。

しかしながら、以下の 3 つの理由により、ミラーリングポートを用いた手法は、家庭内に簡単に導入したいという本研究の目的に合致しない。1 つ目は、ミラーリングポートを備えたスイッチを既存のスイッチに置き換えるだけでなく、ミラーリングポートから出力されたパケットを解析・蓄積するための装置が必要なことである。ホームネットワークが複数のスイッチで構築されていた場合には、スイッチ 1 台につき 1 つのパケット蓄積・解析装置が必要となる。

2 つ目は、有線スイッチのミラーリングポートでは無線 LAN どちらの通信のモニタリングを行うことができないことである。ミラーリングポートを備えた無線 LAN アクセスポイントを導入すれば無線 LAN で通信する DLNA デバイスの通信をもモニタリングすることが可能である。しかしながら、その際には家庭で使用している無線 LAN アクセスポイントの設定をすべてミラーリングポート付きの無線 LAN アクセスポイントに複製する必要がある。

3 つ目は、ミラーリングポートから DLNA デバイス以外のパケットが出力されてしまうことである。すべてのパケットを蓄積するためのストレージ容量が膨大になることや、モニタリングとは個別に DLNA デバイスの IP アドレスや MAC アドレスを調査して DLNA 関連のトラフィックのみを抽出しなければならないなどの問題が発生する。スイッチのフィルタ機能を利用して DLNA デバイスの通信のみをモニタリングすることも可能であるが、DLNA デバイスの MAC アドレスや IP アドレスをあらかじめ登録するといった設定が必要となる。

## 3. DLNA Probe

すでに展開されている DLNA<sup>13)</sup> デバイスに変更を加えることなく操作履歴を取得することを目的として、DLNA デバイス間の通信をモニタリングするシステム「DLNA Probe」の設計を行った。DLNA Probe では SSDP<sup>14)</sup> を用いて DLNA デバイスの IP アドレスと MAC アドレスを取得し、ARP スプーフィングを行って各 DLNA デバイスの ARP テーブルを外部から書き換える。DLNA デバイス間の通信がすべて DLNA Probe 経由になるよ

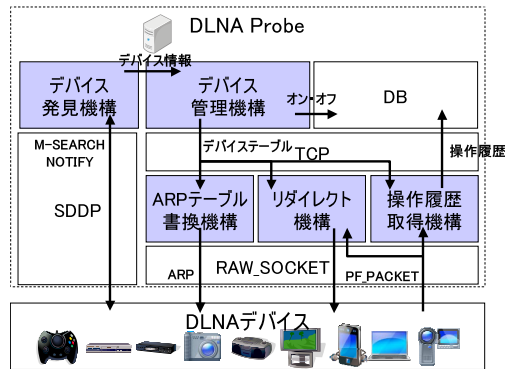


図 1 全体像  
Fig. 1 Overview.

うにリダイレクトすることで DLNA デバイス間の通信をモニタリングする。

このときの ARP スプーフィングでは、DLNA デバイス間の通信のみをリダイレクトするために、ARP スプーフィングを検出されないことと、DLNA デバイス間の通信のみをモニタリング可能であることの 2 つが求められる。このような 2 つの要件に対して、DLNA Probe の ARP スプーフィングでは、通常用いられる ARP リクエストをブロードキャストで送出する方法ではなく、ARP リクエストをユニキャストで送出する方法で実現する。

このような仕組みにより、ユーザは 1 台の DLNA Probe をホームネットワークに追加接続するだけですべての DLNA デバイス間の通信をモニタリングすることができる。DLNA Probe は ARP スプーフィングによるリダイレクトで実現されるため、ホームネットワークが複数の有線スイッチと無線アクセスポイントが混在した環境であっても利用することができる。また、SSDP とユニキャスト ARP リクエストを用いた ARP スプーフィングを組み合わせることにより、事前に各 DLNA デバイスの IP アドレスや MAC アドレスを調べることなしに DLNA デバイス間の通信のみをモニタリングすることができる。

図 1 に DLNA Probe の全体像を示す。DLNA Probe は、デバイス管理機構、デバイス発見機構、ARP テーブル書き換え機構、リダイレクト機構、操作履歴取得機構の 5 つの機構から構成される。

### 3.1 デバイス管理機構

デバイス管理機構はデバイス情報を管理するためのディレクトリサービスである。デバイ

ス管理機構では、デバイス発見機構から送られてくる発見された DLNA デバイスの IP アドレス、MAC アドレス、発見時刻の組を管理し、ARP テーブル書き換え機構、リダイレクト機構、操作履歴取得機構に対して、デバイス情報をデバイステーブルとして提供する。

デバイス管理機構はクライアントサーバ形式のサーバとして構築されており、デバイス発見機構、ARP テーブル書き換え機構、リダイレクト機構、操作履歴取得機構がクライアントとして動作する。デバイス管理機構はクライアントの要求に対して応答を返す要求応答型と、デバイステーブルに変更があった場合にクライアントに対して変更を通知するイベント通知型の 2 種類の動作をする。

要求応答型の動作では、デバイス管理機構内のデバイステーブルのすべての項目を返す LIST コマンド、デバイステーブルに新しいデバイスを追加する ADD コマンド、デバイステーブルからデバイスを削除する DELETE コマンドの 3 つのコマンドをクライアントから受け付ける。イベント通知型の動作では、デバイステーブルに新しい項目を追加された場合に追加された項目を通知する ADDED イベント、デバイステーブルから項目が削除された場合に削除された項目を通知する DELETED イベントの 2 つのイベントをクライアントに対して送信する。

### 3.2 デバイス発見機構

デバイス発見機構は定期的に SSDP を用いてデバイスの発見を行い、デバイス管理機構に対して発見したデバイスを通知する。SSDP は能動的にデバイスを検索する M-SEARCH と呼ばれる機能を備えている。しかしながら、クライアントとして動作する DMC や DMP などのデバイスは実装によっては M-SEARCH に対して返答しない。このような DLNA デバイスを発見するために、デバイス発見機構では、能動的な発見と受動的な発見を組み合わせる。受動的な発見は、DLNA デバイスが定期的に発行する検索メッセージや広告メッセージを監視することによって行う。

能動的な発見では、定期的に M-SEARCH メッセージをマルチキャストすることでデバイステーブルを最新に保つ。M-SEARCH は、SSDP において他の DLNA デバイスを検索するための仕組みである。他のサービスを発見したい場合、端末は M-SEARCH メッセージを HTTPMU (HTTP Multicast over UDP)<sup>39)</sup> で送信する。M-SEARCH を受け取った各端末は ST (search type) ヘッダに記述されたサービスに適合するサービスを持っていた場合にはマルチキャストパケットの送信元アドレスと送信元ポートへと HTTPU (HTTP over UDP)<sup>39)</sup> でレスポンスメッセージを送信する。

図 2 に M-SEARCH メッセージの例を示す。MAN (mandatory) ヘッダには、SSDP に

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
ST: ssdp:all
MX:3
```

図 2 M-SEARCH パケット  
Fig. 2 M-SEARCH packet.

おける発見のためのメッセージであることを意味する `ssdp:discover` が記述されている。ST ヘッダには、検索対象がすべてのサービスであることを意味する `ssdp:all` が記述されている。

M-SEARCH を送るときには、宛先を管理スコープのマルチキャストアドレス 239.255.255.250、宛先ポートを SSDP の 1900、送信元アドレスを自端末のアドレス、送信元ポートを 21400 として投げる。DLNA Probe から M-SEARCH を受け取った DLNA デバイスは、HTTPU でポート 21400 に対して HTTP レスポンスを送信する。DLNA Probe は RAW ソケットを介して 21400 で HTTP レスポンスを受け取ると、HTTP レスポンスパケットに含まれる送信元 IP アドレスと送信元 MAC アドレスを取得し、デバイス管理機構に ADD コマンドを送る。

受動的な発見では、SSDP のポート 1900 に送られてくる M-SEARCH メッセージや、GENA<sup>38)</sup> の NOTIFY メッセージを監視することでデバイスの発見を行う。各 DLNA デバイスは、SSDP の機能により、他のデバイスを発見するための M-SEARCH メッセージや、自分の状態を広告するための NOTIFY メッセージを定期的にマルチキャストアドレス「239.255.255.250」、ポート「1900」に対してマルチキャストする。M-SEARCH メッセージや NOTIFY メッセージを RAW ソケットで受け取った DLNA Probe はメッセージの IP アドレスと MAC アドレスを取得する。NOTIFY メッセージの NTS (notify sub-type) フィールドが DLNA デバイスの離脱を意味する「`ssdp:byebye`」である場合には、デバイス管理機構に対して DELETE コマンドを送信し、NTS フィールドがそれ以外 (たとえば生存を意味する「`ssdp:alive`」) である場合には ADD コマンドを送信する。

### 3.3 ARP テーブル書き換え機構

ARP テーブル書き換え機構は、デバイス管理機構より取得したデバイステーブルの IP アドレスと MAC アドレスを用いてすべての DLNA デバイスに対して ARP スプーフィングを行う。ARP スプーフィングは ARP を詐称して外部から端末の ARP テーブルを書き

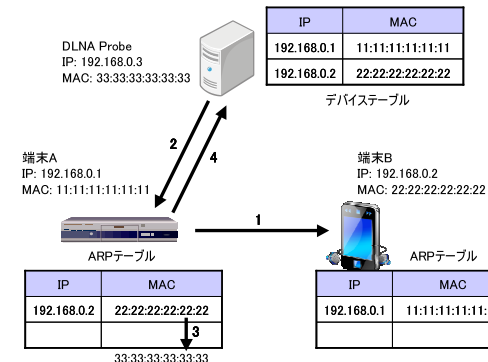


図 3 ARP スプーフィングの動作  
Fig. 3 ARP spoofing.

換える技術である。

図 3 に ARP スプーフィングの動作例として、DLNA Probe が端末 A の ARP テーブルを書き換えて、端末 B に対するパケットを DLNA Probe 宛てに変更する手順を示す。まず、端末 A の ARP テーブルには端末 B の IP アドレス「192.168.0.2」と MAC アドレス「22:22:22:22:22:22」が記録されている。この状態では端末 A が IP アドレス「192.168.0.2」宛てにパケットを送信すると正しい宛先である端末 B にパケットが配信される。次に DLNA Probe が送信元 IP アドレス「192.168.0.2」、送信元 MAC アドレス「33:33:33:33:33:33」の詐称した ARP パケットを端末 A に対して送信する。すると端末 A の ARP テーブルの「192.168.0.2」に対応付けられている MAC アドレスが「33:33:33:33:33:33」に書き換わる。このように ARP テーブルを書き換えることで、端末 A から端末 B へのパケットは DLNA Probe に送信されることになる。

DLNA Probe で ARP スプーフィングを用いる場合、ARP スプーフィングを行っていることの検出されにくさ、書き換え範囲、DLNA Probe が送信するパケット数を考える必要がある。表 1 に 4 種類の ARP スプーフィングの方式を示す。ARP スプーフィングには偽造した ARP リプライをブロードキャストする方法 (ブロードキャスト ARP リプライ)、偽造した ARP リクエストをブロードキャストする方法 (ブロードキャスト ARP リクエスト)、偽造した ARP リプライをユニキャストする方法 (ユニキャスト ARP リプライ)、偽造した ARP リクエストをユニキャストする方法 (ユニキャスト ARP リクエスト) の 4 つが存在する。

表 1 各 ARP スプーフィング手法の比較  
Table 1 Comparison among 4 methods of ARP spoofing.

	ブロードキャスト ARP リプライ	ブロードキャスト ARP リクエスト	ユニキャスト ARP リプライ	ユニキャスト ARP リクエスト
検出されにくさ	×	×	×	
書き換え範囲	全端末	全端末	指定端末	指定端末
DLNA Probe が送信するパケット数	△	△	○	×

ブロードキャスト ARP リプライとブロードキャスト ARP リクエストでは、ブロードキャストを用いてサブネット内のすべての端末の ARP テーブルを 1 度書き換えることができる。そのため、登録されている DLNA デバイスの数だけブロードキャストパケットを送ればよい。

しかしながら、ブロードキャストを用いるので IP アドレスを乗っ取られた端末が IP アドレスが乗っ取られたことを検出してしまふ。たとえば Windows XP では、自分と同じ IP アドレスと自分と異なる MAC アドレスを含む ARP リクエストを受け取った場合、ユーザに対して IP アドレスが重複していることを通知し、ネットワーク機能が無効になる。また、ブロードキャストを用いた手法では ARP を受け取った端末すべての ARP テーブルが書き換えられ、DLNA デバイス以外の端末が送信するパケットもすべて DLNA Probe に送られるという問題が発生する。

ユニキャスト ARP リプライでは、各 DLNA デバイスが送信した ARP リクエストに対応した形で詐称した ARP リプライが送信される。ARP リクエストを監視して必要なときだけ偽造した ARP リプライを送るので、定期的に送る手法に比べて DLNA Probe が送るパケット数を抑えることができる。また、ユニキャストを用いるので、DLNA デバイスのみを指定して ARP スプーフィングを行うことができる。

しかしながら、ARP リクエストを送った端末は、DLNA Probe と正しい端末の 2 つの ARP リプライを受け取る。1 つの ARP リクエストに対する 2 つの ARP リプライの存在は、ネットワーク内に IP アドレスを乗っ取っている端末がいることを ARP リクエストを送信した端末に教えることになる。また、ARP リプライを送るタイミングによっては ARP テーブルを書き換えることができない場合もある。たとえば、Windows XP では、ARP リプライが 2 つ届いた場合には後に届いた ARP リプライで ARP テーブルが書き換えられる。

ユニキャスト ARP リクエストでは、ARP リクエストをユニキャストで送信した宛先の ARP テーブルのみを書き換えることができる。そのため、IP アドレスを乗っ取られた端末

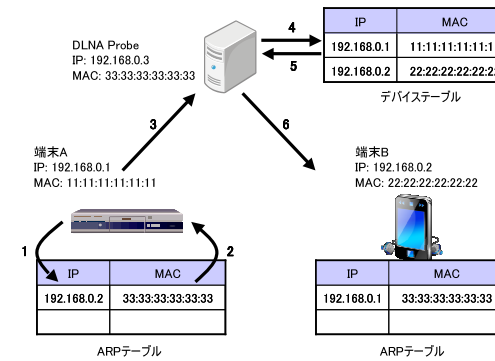


図 4 リダイレクト機構の動作  
Fig. 4 Redirect component.

も、ユニキャスト ARP リクエストを受け取った端末も、IP アドレスが乗っ取られたことを検出できない。一方、ARP テーブルが一定時間経過するとクリアされてしまうため、詐称した ARP リクエストを定期的にする必要がある。また、1 度のユニキャスト ARP リクエストでは 1 つの端末の ARP テーブルの 1 つの項目しか更新することができない。つまり、 $N \times N$  個のユニキャスト ARP リクエストを送信する必要がある。

DLNA Probe では、ARP スプーフィングを検出されないこと、DLNA デバイス間の通信のみをモニタリング可能であることの 2 つの利点より、ユニキャスト ARP リクエストを用いて ARP スプーフィングを行う。

### 3.4 リダイレクト機構

ARP テーブル書き換え機構によってすべての DLNA デバイス間の通信は DLNA Probe へと送信される。リダイレクト機構では、DLNA Probe が受信したパケットの MAC アドレスを正しい MAC アドレスへと書き換えて送信することで正しい宛先へとリダイレクトする。

図 4 を用いて、リダイレクト機構の動作を説明する。まず、リダイレクト機構はデバイス管理機構よりデバイステーブルを取得する。デバイステーブルには端末 A と端末 B の IP アドレスと MAC アドレスが記録されている。端末 A が端末 B にパケットを送信する場合、1) ARP テーブルを参照して端末 B の IP アドレス「192.168.0.2」に対応付けられている MAC アドレスを取得する。2) ARP テーブルは ARP テーブル書き換え機構によって書き換えられているため、取得される MAC アドレスは「33:33:33:33:33:33」とな

る．3) 端末 A は宛先 IP アドレスが「192.168.0.2」, 宛先 MAC アドレスが DLNA Probe の「33:33:33:33:33:33」, 送信元 IP アドレスが端末 A の「192.168.0.1」, 送信元 MAC アドレスが端末 A の「11:11:11:11:11:11」でパケットを送信する．4) パケットを受け取った DLNA Probe は, デバイステーブルを参照して IP アドレス「192.168.0.2」を持つ端末の MAC アドレスを調べる．5) 「192.168.0.2」に対応付けられた MAC アドレスとして「22:22:22:22:22:22」が得られる．6) DLNA Probe は得られた「22:22:22:22:22:22」を宛先 MAC アドレスに設定し, 送信元 MAC アドレスを DLNA Probe の MAC アドレス「33:33:33:33:33:33」に書き換え, ネットワークに送信する．以上の手順で端末 A から送信されたパケットが DLNA Probe を経由して端末 B に到達する．

### 3.5 操作履歴取得機構

DLNA Probe ではユーザが DLNA デバイスの操作履歴を取得することを目的としているため, DLNA デバイスの操作に関連する情報のみをデータベースに保存する．具体的には, リダイレクト機構によってパケットをリダイレクトすると同時に, 操作履歴取得機構でパケットの中身をチェックし, パケット中に DLNA デバイスの操作に関するメッセージが含まれていた場合にはそのメッセージをデータベースへと保存する．DLNA デバイス間でやりとりされるメッセージは HTTP を用いるため, HTTP ヘッダの情報を記録することで DLNA デバイスの操作履歴を取得することができる．

DLNA で扱うメソッドは, ファイルの取得が確認できる GET, コマンドの送信を確認できる POST, ファイルの送信が確認できる PUT の 3 種類のメッセージが存在する．パケットのデータフィールドの先頭が「GET, PUT, POST」のいずれかであった場合には, パケットの宛先アドレスがデバイス管理機構から取得したデバイステーブルに含まれるかどうかをチェックし, パケットのデータフィールドをデータベースに対して書き込む．データベースへは, 送信元 IP アドレス, 宛先 IP アドレス, メソッド名, メッセージが書き込まれる．HTTP リクエスト行は毎回パケットの同じ位置 (TCP データフィールドの先頭) に記述されているため, 最も長い HTTP メソッド「POST」の 4 バイトのメモリ比較演算でメソッドのチェックが実装可能である．

## 4. 実機評価

DLNA Probe の基本性能を評価することを目的として, 実機評価を行った．

### 4.1 実装

DLNA Probe を評価するために, 実装を行った．CPU が 2.26 GHz のインテル Core2Duo

表 2 実装したプログラムのバイナリサイズ, 使用メモリ量  
Table 2 Footprint and memory usage of implemented components.

機構名	プログラム名	バイナリサイズ (バイト)	使用メモリ量 (バイト)
デバイス管理機構	dlnap_directory	19,565	1,098
デバイス発見機構	dlnap_discovery	14,306	441
ARP テーブル書き換え機構	dlnap_spoofeer	19,444	442
リダイレクト機構	dlnap_router	19,388	442
操作履歴取得機構	dlnap_logger	24,383	1,100
合計		97,086	3,523

The screenshot shows a web browser window with the title "DLNA Probe". The main content area is divided into two sections: "DLNA DEVICE LIST" and "OPERATION HISTORY".

**DLNA DEVICE LIST**

IP	MAC	Name
192.168.11.1	00:1d:73:c8:33:e8	router
0.0.0.0	00:24:be:94:2f:83	
192.168.11.3	00:24:be:63:96:a2	NetJuke

**OPERATION HISTORY**

```

2010-07-24 00:04:27 192.168.11.2 192.168.11.3 POST:DIRECTORY
2010-07-24 00:04:27 192.168.11.2 192.168.11.3 GET:FILE
2010-07-24 00:04:27 192.168.11.2 192.168.11.3 GET:FILE
2010-07-24 00:04:27 192.168.11.2 192.168.11.3 GET:FILE
2010-07-24 00:04:27 192.168.11.2 192.168.11.3 POST:DIRECTORY
2010-07-24 00:04:56 192.168.11.2 192.168.11.2 SYSTEM:OFF
2010-07-24 00:20:12 192.168.11.4 192.168.11.4 SYSTEM:OFF
2010-07-24 00:21:36 192.168.11.4 192.168.11.4 SYSTEM:ON
2010-07-24 00:26:37 192.168.11.4 192.168.11.4 SYSTEM:OFF

```

図 5 スクリーンショット

Fig. 5 Screenshot.

プロセッサ P8400, メモリが 1 GB の Lenovo X200 上で, Linux 2.6.27-17, Apache 2.2.9, MySQL 5.0.67, PHP 5.2.6 を用いて実装を行った．表 2 に実装したプログラムのバイナリサイズと使用メモリ量を示す．DLNA Probe は C 言語を用いて実装し, 5 つのプログラムに分割した．デバイス管理機構 (dlnap\_directory) と操作履歴取得機構 (dlnap\_logger) は MySQL とデータのやりとりをするため, 使用メモリ量が他のプログラムに比べて大きい．デバイス発見機構では, 30 秒ごとに M-SEARCH パケットを送信するように設定している．ARP テーブル書き換え機構では, 30 秒ごとに ARP リクエストパケットを送出している．また, 操作履歴を確認するためのログビューアを PHP を用いてウェブサービスとして実装した．図 5 に実装したログビューアのスクリーンショットを示す．ログビューアでは, MySQL からデータを読み出し, 現在起動中の DLNA デバイスのリストと, 操作履歴を閲

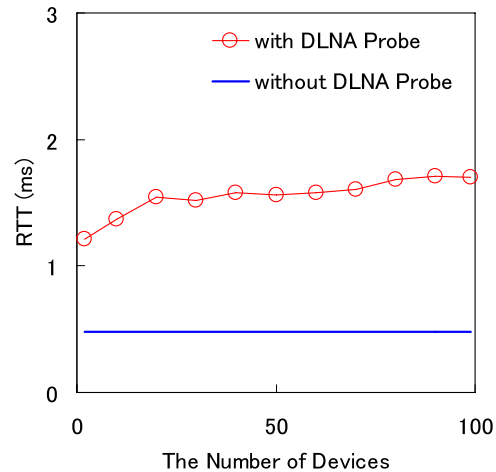


図 6 デバイス数に応じた平均遅延

Fig. 6 Average delay vs. the number of devices.

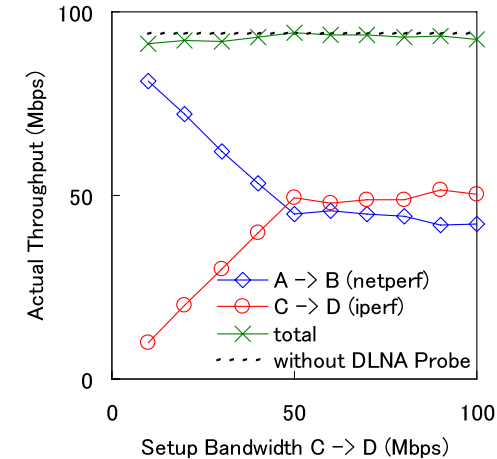


図 7 2つのフローのスループット

Fig. 7 Throughput of two flows.

覧することができる。デバイスのリストと操作履歴は Ajax を用いてリアルタイムに更新される。

#### 4.2 評価

DLNA Probe が DLNA<sup>13)</sup> デバイス間の通信に与える通信遅延とスループットに与える影響の評価を行った。検証環境として、100 Mbps のスイッチングハブに仮想 DLNA デバイスを接続して計測を行った。

##### 遅延

DLNA における著作権保護技術である DTCP-IP<sup>15)</sup> の要求遅延が 7 ms 以下であるため、DLNA Probe によって生じる遅延も 7 ms 以下に抑える必要がある。遅延の評価は、ping を用いて DLNA Probe が存在する場合、存在しない場合の RTT (Round Trip Time) の計測を行った。

図 6 にデバイス数に応じた平均遅延を示す。横軸がデバイス数で縦軸が平均遅延である。図 6 から分かるように、DLNA Probe を用いた場合では、平均で約 1 ms の遅延が増加する。この 1 ms の遅延は、DLNA Probe の処理遅延である。また、デバイス数を増やすにつれて遅延が増加しており、デバイス数 100 台のときは 1.6 ms の平均遅延が発生している。この遅延の増加は、ARP スプーフィングのトラフィックがデバイス数の増加によって増え

ることで、ユニキャスト ARP リクエストパケットが送られるタイミングで遅延を計測する機会が増加することに起因する。

##### スループット

DLNA では動画の転送などを行うため、DLNA Probe のリダイレクト処理や操作履歴取得処理によってスループットが著しく低下することは避けなければならない。

まず、A, B, C, D とラベル付けされた端末 4 台を用いて、netperf と iperf で計測を行った。端末 4 台間の通信はすべて DLNA Probe を経由する。A から B への通信は netperf を用いて TCP の実行スループットを計測し、C から D への通信は iperf を用いて一定の帯域の UDP トラフィックを流した。

図 7 にスループットの計測結果を示す。iperf の設定トラフィックが 50 Mbps になるまでは C から D への通信は設定どおりのスループットが観測されたが、A から B のスループットは C から D のトラフィックが増えるに従って減少した。iperf の設定トラフィックが 50 Mbps を超えると、A から B への実効スループットと C から D への実効スループットがともに 50 Mbps 前後となった。すべての場合において A から B へのスループットと C から D へのスループットの合計が DLNA Probe がいない場合の最大スループットである約 94 Mbps を超えることはなかった。これは、すべてのトラフィックが DLNA Probe を経由



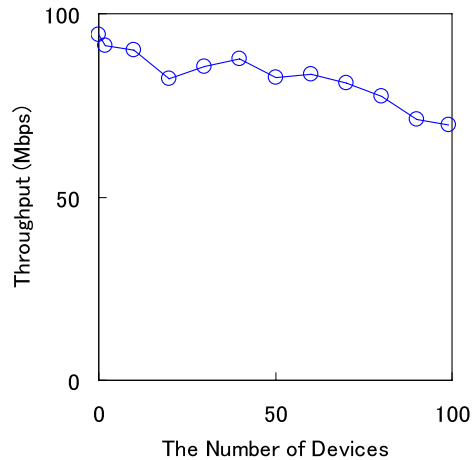


図 8 デバイス数に応じたスループット  
Fig. 8 Throughput vs. the number of devices.

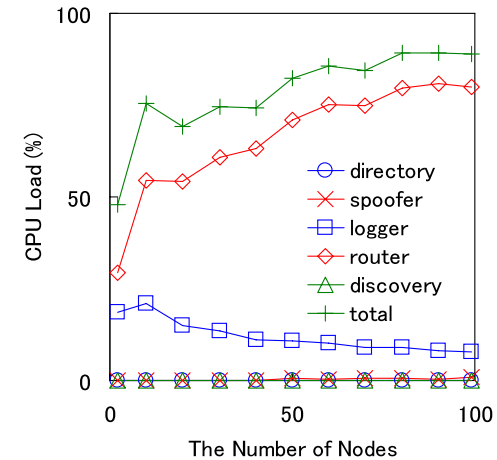


図 9 デバイス数に応じた CPU 負荷  
Fig. 9 CPU load vs. the number of devices.

するため、すべてのスループットの合計が DLNA Probe が持つリンク速度に制限されることに起因する。また、すべてのスループットの合計は DLNA Probe がない場合のスループットである約 94 Mbps とほぼ同じであった。これは DLNA Probe の処理が DLNA デバイス間の通信のスループットに与える影響がほとんどないことを意味している。

次に、DLNA デバイス数の増加がスループットに与える影響の評価を netperf を用いて行った。図 8 に DLNA デバイスの数を変化させたときの、2 台の DLNA デバイス間のスループットを示す。横軸がデバイス数で、縦軸がスループットを意味する。DLNA デバイスの数が増えるに従い、スループットが低下していく。

デバイス数が増えた場合にスループットが下がる原因を突き止めるために、各機構の CPU 負荷を計測した。図 9 にデバイス数を変化させたときのデバイス管理機構 (directory)、デバイス発見機構 (discovery)、ARP テーブル書き換え機構 (spoofers)、リダイレクト機構 (redirect)、操作履歴取得機構 (logger) の CPU 負荷の計測結果を示す。デバイス数が増えるに従い、パケットをリダイレクトするリダイレクト機構の CPU 負荷が著しく増加していることが分かる。これはパケットが来るたびに、デバイステーブルを参照して IP アドレスと MAC アドレスを検索するため、デバイステーブルのサイズが大きくなると IP アドレスと MAC アドレスを検索するオーバーヘッドが大きくなることに起因する。

```
POST /control/ContentDirectory HTTP/1.1
X-AV-Physical-Unit-Info: pa="XX";
X-AV-Client-Info: av=5.0; cn="XX"; mn="XX"; mv="X.X";
Host: 192.168.11.11:30000
User-Agent: UPnP/1.0 DLNADOC/1.50
Content-Length: 650
Content-Type: text/xml; charset="utf-8"
SOAPACTION: "urn:schemas-upnp-org:service:ContentDirectory:1#Browse"
```

図 10 ディレクトリ閲覧時の POST メソッド  
Fig. 10 POST method when browsing a directory.

#### 取得した操作履歴

実装した DLNA Probe を実際の家庭内に設置し、DLNA デバイスの操作履歴の取得を行った。まず、コンテンツ閲覧に関する情報の抽出を操作履歴を用いて行った。図 10 にコンテンツを選択するためのディレクトリ閲覧時の POST メソッドを示す。POST メソッドでは、ヘッダの SOAPACTION フィールドを参照することで SOAP を用いたディレクトリ閲覧

```

GET /2424-2430.mpg HTTP/1.1
TimeSeekRange.dlna.org: npt=0.000-
getContentFeatures.dlna.org: 1
Pragma: getIfoFileURI.dlna.org
transferMode.dlna.org: Streaming
X-AV-Physical-Unit-Info: pa="XX";
X-AV-Client-Info: av=5.0; cn="XX"; ...
Host: 192.168.11.11:30001

```

図 11 再生時の GET メソッド

Fig. 11 GET method when playing a content.

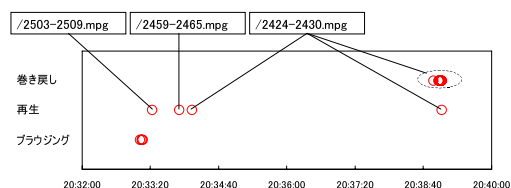


図 12 DMP から DMS へのアクセス情報

Fig. 12 Access data from DMP to DMS.

の操作を検出できる。図 11 にコンテンツ再生時の GET メソッドを示す。まず、GET の引数でどのコンテンツを再生したかが分かる。この例では /2424-2430.mpg を再生したことが分かる。また、TimeSeekRange.dlna.org フィールドを参照することでコンテンツのどの時点の開始なのか、早送りなのか、巻き戻しなのかが分かる。たとえばコンテンツ冒頭からの再生時には TimeSeekRange.dlna.org フィールドにはコンテンツ冒頭を表す ntp=0.000- が書き込まれている。早送りや巻き戻し時には TimeSeekRange.dlna.org フィールドに ntp=220.547-221.547 などのコンテンツの途中を表す値が書き込まれている。連続した GET メソッドの TimeSeekRange.dlna.org フィールドの ntp の値が増えているか減っているかを判別することで早送りと巻き戻しの区別をすることもできる。

図 12 に DMP から DMS (Digital Media Server) に接続して動画を閲覧した際の操作履歴を示す。操作履歴の抽出では、前述した HTTP ヘッダの情報を利用した。ユーザが DMP のディレクトリを閲覧した後、複数のコンテンツを再生している。また、再生した最後のコンテンツは閲覧後に巻き戻し、途中から再生している。このような家庭内でのコンテンツ閲

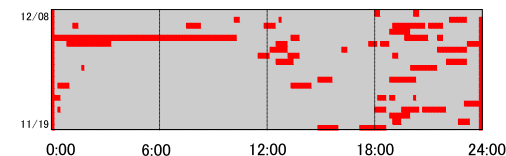


図 13 DMP 機能を備えたテレビの ON/OFF 情報

Fig. 13 DMP equipped TV ON/OFF data.

覧の情報はトラフィックに応じてネットワーク構成を動的に変更することで省電力化を実現する研究<sup>17)</sup> の評価データとして使用できる。

次に、操作履歴から DLNA デバイスの ON/OFF 情報を抽出できることを確認した。図 13 に DMP 機能を備えたテレビの ON/OFF 情報を示す。毎日 24 時になると番組表を受信するために一時的に ON になっていることが分かる。また、12 月 3 日にはテレビを消し忘れたために夜中から昼ごろまでテレビが ON にされたままであることが分かる。これらの ON/OFF 情報は家電の自動電源制御の研究<sup>16)</sup> や、テレビの消し忘れなどの異常状態を検出するためのアルゴリズムの研究<sup>18)</sup> に役立てることができる。

## 5. おわりに

本論文では、DLNA デバイスの操作履歴を取得するシステム、DLNA Probe の設計、実装、評価について述べた。DLNA Probe では、SSDP と ARP スプーフィングを組み合わせることで、既存の DLNA の枠組みを壊すことなく DLNA デバイスの操作履歴を取得可能であることを示した。また、DLNA デバイスの操作履歴を取得する際の ARP スプーフィングでは、ターゲットノードに対してユニキャストで ARP リクエストを送る手法が有効であることも示した。DLNA Probe を実装して評価した結果では、DLNA の著作権保護技術である DTCP-IP の要求遅延 7ms を満たすことと、DLNA Probe の処理がスループットにほとんど影響を与えないことが確認された。

## 参考文献

- 1) Zancanaro, M., Kuflik, T., Boger, Z., Goren-Bar, D. and Goldwasser, D.: Analyzing Museum Visitors' Behavior Patterns, *Proc. 11th International Conference on User Modeling (UM'07)*, Corfu, Greece, pp.238-246 (2007).
- 2) Intille, S.S., Larson, K., Tapia, E.M., Beaudin, J.S., Kaushik, P., Nawyn, J. and Rockinson, R.: Using a Live-In Laboratory for Ubiquitous Computing Re-

- search, *Proc. 4th International Conference on Pervasive Computing (Pervasive'06)*, Dublin, Ireland (2006).
- 3) Tapia, E.M., Intille, S.S., Lopez, L. and Larson, K.: The Design of a Portable Kit of Wireless Sensors for Naturalistic Data Collection, *Proc. 4th International Conference on Pervasive Computing (Pervasive'06)*, Dublin, Ireland (2006).
  - 4) Mozer, M.C.: The Neural Network House: An Environment that Adapts to its Inhabitants, *Proc. American Association for Artificial Intelligence Spring Symposium*, Menlo Park, Canada, pp.110–114 (1998).
  - 5) Kim, Y., Schmid, T., Charbiwala, Z.M., Friedman, J. and Srivastava, M.B.: NAWMS: Nonintrusive Autonomous Water Monitoring System, *Proc. 6th ACM Conference on Embedded Networked Sensor Systems (SenSys'08)*, Raleigh, North Carolina, pp.309–322 (2008).
  - 6) Olguin, D.O.: Sociometric Badges: Wearable Technology for Measuring Human Behavior, Master's thesis, Massachusetts Institute of Technology (2007).
  - 7) Yamazaki, T.: Ubiquitous Home: Real-life Testbed for Home Context-aware Service, *Proc. 1st International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (Tridentcom'05)*, Trento, Italy, pp.54–59 (2005).
  - 8) Kidd, C.D., Orr, R., Abowd, G.D., Atkeson, C.G., Essa, I.A., MacIntyre, B., Mynatt, E., Starner, T.E. and Newstetter, W.: The Aware Home: A Living Laboratory for Ubiquitous Computing Research, *Proc. 2nd International Workshop on Cooperative Buildings. Integrating Information, Organizations and Architecture (CoBuild'99)*, Pittsburgh, Pennsylvania, pp.191–198 (1999).
  - 9) 矢野和男 : センサは Web を超える : 省力化から知覚化へ , *情報処理* , Vol.48, No.2, pp.160–170 (2007).
  - 10) Jiang, X., Ly, M.V., Taneja, J., Dutta, P. and Culler, D.: Experiences with A High-Fidelity Wireless Building Energy Auditing Network, *Proc. 7th ACM Conference on Embedded Networked Sensor Systems (SenSys'09)*, Berkeley, California (2009).
  - 11) ECHONET Consortium: ECHONET Specification. <http://www.echonet.gr.jp>
  - 12) Gu, T., Pung, H.K. and Zhang, D.Q.: Towards an OSGi-Based Infrastructure for Context-Aware Applications, *IEEE Pervasive Computing*, Vol.3, No.4, pp.66–74 (2004).
  - 13) Digital Living Network Alliance. <http://www.dlna.org>
  - 14) Goland, Y., Cai, T., Leach, P. and Gu, Y.: Simple Service Discovery Protocol, Internet Draft (2000).
  - 15) Digital Transmission Licensing Administrator: *DTCP Volume 1 Supplement E Revision 1.2 (Informational Version)* (2007). <http://www.dtcp.com/>
  - 16) Si, H., Saruwatari, S., Minami, M. and Morikawa, H.: A Ubiquitous Power Management System to Balance Energy Saving and Response Time based on Device-level Usage Prediction, *Journal of Information Processing*, Vol.18, pp.147–163 (2010).
  - 17) Nguyen, P.L., Morohashi, T., Imaizumi, H. and Morikawa, H.: A Performance Evaluation of Energy Efficient Schemes for Green Office Networks, *Proc. 2nd IEEE Green Technologies Conference*, Grapevine, Texas (2010).
  - 18) Baek, S., Si, H., Saruwatari, S., Morikawa, H., Hjelm, J. and Oda, T.: Anomaly Detection from the Operation History of DLNA Devices, *Proc. 2nd International Conference on Ubiquitous and Future Networks (ICUFN'10)*, Jeju Island, Korea, pp.390–393 (2010).
  - 19) 丹 康雄 : ホームネットワーク (OSGi, ECHONET) モデルに基づく家庭内エネルギーマネジメント , *情報処理* , Vol.51, No.8, pp.959–965 (2010).
  - 20) Song, T.Y., Kawahara, Y. and Asami, T.: Using SNS as Access Control Mechanism for DLNA Content Sharing System, *Proc. 6th IEEE Consumer Communications and Networking Conference (CCNC'09)*, Las Vegas, Nevada, pp.1–2 (2009).
  - 21) Belimpasakis, P., Michael, M.P. and Moloney, S.: The Home as a Content Provider for Mash-ups with External Services, *Proc. 6th IEEE Consumer Communications and Networking Conference (CCNC'09)*, Las Vegas, Nevada (2009).
  - 22) Cagenius, T., Fasbender, A., Hjelm, J., Horn, U., Ivars, I.M. and Selberg, N.: Evolving the TV experience: Anytime, anywhere, anydevice, *Ericsson Review*, No.3, pp.107–111 (2006).
  - 23) Gallego, I.L., Garcia, F.R., Valverde, J.M.P., Rizaldos, J.L. and Vidal, F.G.: DLNA-based IPTV Platform, *Proc. 6th IEEE Consumer Communications and Networking Conference (CCNC'09)*, Las Vegas, Nevada (2009).
  - 24) Oh, Y.J., Lee, H.K., Kim, J.T., Paik, E.H. and Park, K.R.: Design of an Extended Architecture for Sharing DLNA Compliant Home Media from Outside the Home, *IEEE Trans. Consumer Electronics*, Vol.53, No.2, pp.542–647 (2007).
  - 25) Lee, H.Y. and Kim, J.W.: An Approach for Content Sharing among UPnP Devices in Different Home Networks, *IEEE Trans. Consumer Electronics*, Vol.53, No.4, pp.1419–1426 (2007).
  - 26) Motegi, S., Tasaka, K., Idoue, A. and Horiuchi, H.: Proposal on Wide Area DLNA Communication System, *Proc. 5th IEEE Consumer Communications and Networking Conference (CCNC'08)*, Las Vegas, Nevada (2008).
  - 27) Haruyama, T., Mizuno, S., Kawashima, M. and Mizuno, O.: Dial-to-Connect VPN System for Remote DLNA Communication, *Proc. 5th IEEE Consumer Communications and Networking Conference (CCNC'08)*, Las Vegas, Nevada (2008).
  - 28) Hwang, T., Park, H. and Chung, J.W.: Personal Mobile A/V Control Point for Home-to-Home Media Streaming, *Proc. IEEE International Conference on Consumer Electronics (ICCE'08)*, Las Vegas, Nevada (2008).

- 29) 小山卓視, 吳 敬源, 武藤大悟, 吉永 努: Mobile-Wormhole Device : DLNA 情報家電の相互遠隔接続支援機構の携帯端末への応用, 情報処理学会研究報告, MBL, pp.1-8 (2008).
- 30) Venkitaraman, N.: Wide-Area Media Sharing with UPnP/DLNA, *Proc. 5th IEEE Consumer Communications and Networking Conference (CCNC'08)*, Las Vegas, Nevada, pp.294-298 (2008).
- 31) Belimpasakis, P., Moloney, S., Stirbu, V. and Requena, J.C.: Home Media Atomizer: Remote Sharing of Home Content – without Semi-trusted Proxies, *IEEE Trans. Consumer Electronics*, Vol.54, No.3, pp.1114-1122 (2008).
- 32) Wu, S.C., Ku, Y.C. and Lee, T.L.: Zero-Configuration Personal Firewall for DLNA DMS, *Proc. IEEE Asia-Pacific Services Computing Conference (APSCC'08)*, Yilan, Taiwan, pp.847-850 (2008).
- 33) Miyake, M., Yoshikawa, T. and Takeshita, A.: Technology for Controlling Access to Content between Different Home Networks, *NTT DOCOMO Technical Journal*, Vol.10, No.3, pp.37-43 (2008).
- 34) Setten, M., Pokraev, S. and Koolwaaij, J.: Context-Aware Recommendations in the Mobile Tourist Application COMPASS, *Adaptive Hypermedia 2004*, Eindhoven, Netherlands, pp.235-244 (2004).
- 35) Kawahara, Y., Kurasawa, H. and Morikawa, H.: Recognizing User Context Using Mobile Handsets with Acceleration Sensors, *Proc. IEEE Portable*, Orland, FL, pp.1-5 (2007).
- 36) 田村 大: ビジネス・エスノグラフィ: 機会発見のための質的リサーチ, 計測と制御, Vol.48, No.5 (2009).
- 37) UPnP Forum: *UPnP Device Architecture 1.0* (2003).
- 38) Cohen, J. and Aggarwal, S.: General Event Notification Architecture Base, Internet Draft (1999).
- 39) Goland, Y.Y.: Multicast and Unicast UDP HTTP Messages, Internet Draft (1999).

(平成 22 年 7 月 28 日受付)

(平成 23 年 1 月 14 日採録)

## 推薦文

本論文では, DLNA デバイスの操作ログを用いてリコメンドサービスなどを行うために, DLNA デバイスの操作履歴を取得する方式について提案と実装を行っている. 提案手法は, 既存の ARP SPOOFING によるスニファの仕組みを活用しているものだが, 既存 DLNA 機器への変更を必要としないという現実的な制約条件の下で, 目的を実現するためのアプローチが明確に記述されており, 論文誌に値する有用性を持つ研究と考える. 構成, 関連研

究との比較も十分であり, かつ提案方式を実装・評価を行っていることも高く評価できる. 今後の操作ログ取得・利用の研究の発展に寄与すると考えられるので, 本論文を推薦論文として推薦する.

(モバイルコンピューティングとユビキタス通信研究会主査 竹下 敦)



猿渡 俊介 (正会員)

2007 年東京大学大学院博士課程修了. 2003~2004 年 IPA 未踏ソフトウェア創造事業, 2006~2008 年日本学術振興会学振特別研究員, 2007~2008 年イリノイ大学客員研究員, 現在, 東京大学先端科学技術研究センター助教. 専門はワイヤレスネットワーク, センサネットワーク, システムソフトウェア等. 2009 年電子情報通信学会論文賞. 2010 年情報処理学会山下記念研究賞. 電子情報通信学会, IEEE, ACM 各会員.



ヨハン イェルム

ウプサラ大学卒業後, Bonniers 社にて報道記者, 編集長, 研究リーダー. 1996 年エリクソンリサーチに入社. OMA, W3C 等の標準化に参加. マサチューセッツ工科大学にて客員エンジニア. 2012 年国際会議 Mobile Data Management のインダストリ・トラック共同議長.



小田 稔周

現在, 日本エリクソン(株)エリクソンリサーチジャパン所長. 旧 KDD 研究所にてネットワーク設計, ネットワーク・サービス等の研究開発に従事するとともに, ITU-T SG2 にてトラヒック工学のラポータ, 作業部会副議長を担当. その後, 2000 年に日本エリクソン(株)に入社. マーケットサポート・先端技術部長を経て, 2005 年より現職. 博士(工学). 1998, 1999 年電子情報通信学会論文賞, 2004 年 TTC 功労賞, 等. 著書に, ワイヤレスブロードバンド教科書(共著), IMS 入門(共著), ほか. 電子情報通信学会, IEEE 各会員.



森川 博之 (正会員)

1987年東京大学工学部電子工学科卒業．1992年同大学院博士課程修了．  
1997～1998年コロンビア大学客員研究員．2002～2006年情報通信研究  
機構モバイルネットワークグループリーダー兼務．現在，東京大学先端科  
学技術研究センター教授．専門はコピキタスネットワーク，モバイルコン  
ピューティング，ワイヤレスネットワーク，フォトニックインターネット  
等．本会論文賞，電子情報通信学会論文賞（3回），志田林三郎賞，情報通信月間推進協議会  
情報通信功績賞，ドコモモバイルサイエンス賞等受賞．電子情報通信学会フェロー．IEEE，  
ACM，ISOC，映像情報メディア学会各会員．

---