情報処理学会論文誌　Vol. 49　No. 12　3985–3996 (Dec. 2008)

ルールベースアクセス制御機能を持つ DLNA 情報家電の遠隔共有支援機構

武藤大悟[†1]　吉永努[†1]

我々は，DLNA 機器の接続範囲をホームネットワーク内から宅外・家庭間に拡張することを支援するワームホールデバイスと呼ぶソフトウェアを開発した．ワームホールデバイスは，既存の DLNA 機器および家庭用 UPnP ルータとの接続性を持つとともに，SIP サーバを利用してホームネットワーク間の接続を一括して行う．また，ユーザの設定したルールに基づいて DLNA 機器やコンテンツのアクセス制御を実現する．市販の DLNA 機器や家庭用 UPnP ルータ，家庭向けインターネット接続サービスを用いた複数のホームネットワーク環境を構築し，相互接続とコンテンツ共有に関する実験を行った．その結果，実用的な遅延時間で遠隔接続とアクセス制御を実現できることが分かった．

Remote Sharing Support for DLNA Appliances with Rule-based Access Control Functions

Daigo Muto[†1] and Tsutomu Yoshinaga[†1]

We developed a software named wormhole device (WD) which supports remote connection of DLNA equipment between two home networks. WD has interoperability with existing DLNA products and household UPnP broadband routers. It utilizes a SIP server to establish remote connection with assisting NAT-Traversal for popular home network environments. It also supports access control functions to share remote DLNA equipments and their contents based on rules which are specified by users. We constructed experiments simulating home networks that are connected to the internet through commercial network providers and using different DLNA-enable device for each home. The experiments examined both remote connection and contents sharing. We show the results that WD realizes safe and easy remote contents sharing as well as access control with acceptable latency.

1. はじめに

近年，情報家電の普及はめざましく，なかでも DLNA ガイドライン[1] に準拠した機器が注目されている．DLNA ガイドラインは，情報家電・携帯端末の通信プロトコル，メディアフォーマットなどを標準化することにより，各機器がネットワークを通じて連携動作する仕組みを規定する．しかし，その連携動作の仕組みは単一家庭内の LAN で接続できる範囲のみに限定されており，宅外，家庭間に拡張することは容易でない．

一方で，一般家庭には FTTH や ADSL などのブロードバンド常時接続インターネット環境が普及している．したがって，ホームネットワークに参加する機器が家庭向け NAT ルータ[2] を通してインターネットにアクセスする基盤は整っている．また，持ち運び可能な携帯機器も，第三世代携帯電話や PHS 網，無線 LAN ホットスポットなどによって宅外でもインターネットへの高速な常時接続が可能になってきた．

インターネットに接続でき，宅内外に偏在する情報家電・携帯機器を，相互に接続し連携動作させることができるネットワーク環境は，ユーザの利便性を大きく向上させると期待されている．たとえば，自宅の HDD/DVD レコーダのコンテンツを外出先で携帯電話から見たり，自宅の HDD/DVD レコーダのコンテンツを友人宅のテレビに映して一緒に鑑賞したりする，といったシナリオを実現するものである．

我々は，DLNA 遠隔接続を支援するワームホールデバイス（WD）と呼ぶソフトウェアを開発した[3]．WD は，DLNA 機器が備える設定の簡易さ，操作の一貫性，利用の安全性などを損なわずに，その利用を宅外・ホームネットワーク間へ拡張する．WD をホームサーバなどの家庭内のいずれかの機器で動作させることにより，簡易な操作で安全に DLNA 機器どうしの宅外暗号化通信を可能とする．また，WD はユーザ設定ルールに基づく DLNA 機器やコンテンツへのアクセス制限を実現する．市販の DLNA 情報家電，家庭用 NAT ルータ，および家庭用インターネット接続サービスを利用する複数のホームネットワーク実験環境を構築し，相互接続実験を行った．その結果，DLNA 機器なみに設定・操作が簡単なアクセス制御機能を実現でき，通信遅延も実用上問題ないことを確認した．

以降，2 章で DLNA の概要を説明した後，3 章で関連研究についてまとめる．4 章で提案する WD を説明し，5 章では WD の特徴であるアクセス制御機能について述べる．6 章で

†1 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, University of Electro-Communications

WD の実装と評価を示し，7 章で本論文をまとめる．

2. DLNA の概要

DLNA ガイドラインは，異なる製造元，OS，様々な種類の情報家電が，従来の家電なみの簡単な操作で連携動作を行えるように策定された[4]．この中では，AV コンテンツを蓄積・提供する DMS（Digital Media Server）と，このコンテンツを再生する DMP（Digital Media Player）などが規定されている．また，DMP の代わりに DMR（Digital Media Renderer）を再生に用い，その操作を DMC（Digital Media Controller）から行う利用方法も規定されている．DMS，DMP，DMR，DMC のいずれもネットワークには Ethernet を使用し，基本的な通信プロトコルには UPnP[5] と HTTP を指定している．

UPnP は，主に (1) 機器検出，(2) 機器情報の交換，(3) 機器間のコマンド送信，(4) イベントの監視と通知，などの機能を機器どうしで半自動的に行うためのプロトコルである．具体的には，それぞれ (1) SSDP（Simple Service Discovery Protocol），(2) HTTP-GET メソッドによる XML 交換，(3) SOAP（Simple Object Access Protocol），(4) GENA（Generic Event Notification Architecture）が使用される．また DLNA ガイドラインでは，コンテンツの伝送に HTTP-GET メソッドを用い，DMS，DMP での対応が必須となっている．

これらの機能によって，DLNA 機器をネットワークにつなぐだけで半自動的に設定と利用が可能となり，ユーザはネットワークに関する特別な知識を必要としない．

3. 関 連 研 究

情報家電を宅内で利用するだけでなく，インターネットを介して他のネットワーク上の端末からも利用するための方式がいくつか提案されている．Siphnos は，UPnP フレームワークの SSDP に相当する機能を SIP（Session Initiation Protocol）[6] を利用して再設計し，宅内，宅外から情報家電へのアクセスをシームレスに実現する提案である[7]．ただし，個々の機器にその要求仕様を満たす実装を行う必要があり，既存の DLNA 機器と接続互換性を持たない．

DLNA Media Proxy Server は，宅外から宅内の DLNA 機器への通信を中継する[8]．また，それにアクセスする SIP UA（User Agent）端末の DLNA Media Agent も提案されている．これらは，通信を中継する際に必要なネットワーク間での SSDP や SOAP のプライベートアドレス書き換えなどを行う．ただし，宅内の DMS に対して宅外からアクセスするには DLNA Media Agent に頼ることとなり，従来の DMP が使えないという問題がある．また，コンテンツ転送に利用する HTTP-GET 通信が宅外から宅内 DLNA 機器へ直接接続する方式であり，多くの DMS がセキュリティのため接続を拒否する問題がある．

W-DLNA ゲートウェイは，SIP を利用して家庭間の DLNA 機器連帯動作を行う[9]．ホームネットワーク上では NAT ルータに W-DLNA ゲートウェイを実装し，SOAP メッセージ内のアドレスの書き換えを実現する．このため，W-DLNA ゲートウェイを導入するには既存の NAT ルータを置き換えなくてはならない．

DLNA-ALG Server も W-DLNA ゲートウェイと同様に NAT ルータを置換する中継装置である[10]．インターネット上から DLNA Agent と呼ばれる機器を使って DLNA-ALG Server へ SIP 経由でアクセスすることにより，家庭内の DLNA 機器と接続する．SOAP 通信は，DLNA-ALG Server によって SIP メッセージに変換され DLNA Agent に送信される．この変換のための遅延が，リアルタイム性の高い操作である DMS コンテンツ一覧取得の場合にも 100 個の要素を含むリストに対して 16 秒程度発生すると報告されている．

また以上の関連研究では，DLNA 機器・DMS 内のコンテンツに対してユーザが宅外からのアクセスを選択的に制限する方法が示されていない．本論文で提案する WD は，既存の DLNA 機器，家庭用 NAT ルータと親和性が高く，機器単位やコンテンツ単位でのアクセス制御機能を提供することを特徴とする．

4. ワームホールデバイスの提案

WD の主な機能は以下のとおりである．

- DLNA 機器の宅外・家庭間接続（NAT 透過機能を含む）
- SIP UA としての動作，および SIP 用いた接続先 WD のロケーション解決
- 自ホームネットワーク内の DLNA 機器一覧の作成，他 WD との交換
- UPnP Proxy 機能とアクセス制御
- コンテンツ転送のバッファリング

以下，WD の設計方針と各機能について説明する．

4.1 設 計 方 針

WD の導入目的は，DLNA 機器の宅外・家庭間接続を実現することである．接続の対象とする DLNA ガイドライン準拠機器であれば，新たに機能を追加する必要はなく，既存の機器を使用することができるようにする．ホームネットワーク環境は，現在主流となっている NAT を利用してインターネットに接続する IPv4 環境に対応する．

DLNA 機器は，一般的な家電と同様な操作感で利用できるように設計されている．した

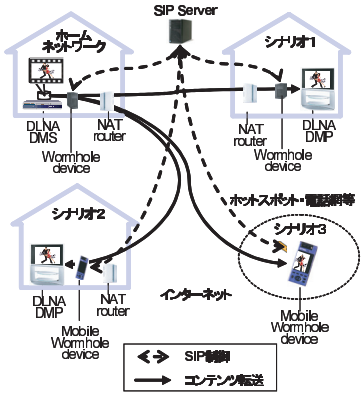

図 1　ワームホールデバイスの構成とシナリオ
Fig. 1　Architecture of wormhole device and its scenarios.

がって，WD も DLNA 機器と同様の導入・設定の簡易さを実現する．具体的には，電源を投入すれば特別な設定なしに利用可能な状態になること，接続先の指定は電話番号程度の入力とすること，通信の暗号化・機器へのアクセス制御はデフォルトの状態で安全な状態を提供できること，かつユーザが簡単に設定変更できること，を基本方針とする．

4.2　ワームホールデバイスが実現するシナリオ

図 1 に，WD が実現する 3 つのシナリオを示す．シナリオ 1 と 2 は自宅の DMS のコンテンツを異なる家庭の DMP で再生するシナリオである．シナリオ 1 では，据置型の WD を利用し，ホームネットワーク間のコンテンツ共有を実現する．たとえば，祖父母宅の DMP で息子宅の DMS に保存されたビデオを視聴する，といったシーンなどが考えられる．

シナリオ 2 では，WD はスマートフォン，無線 LAN 搭載 PDA のような持ち運び可能なデバイス上で動作する．これを持って WD のない家庭に移動し，宅間のコンテンツ共有を実現する．たとえば，友人宅に遊びに行った際に，自宅のコンテンツを友人宅のテレビで一緒に鑑賞する，などのシーンが考えられる．このとき，友人宅のネットワーク機器にはいっさい変更を加えない．

シナリオ 3 は，WD と DMP 機能が搭載された端末で，宅内の DMS 上のコンテンツを楽しむ場合を示す．たとえば，スマートフォンを使って電車移動中に自宅の DMS に記録した動画を視聴する，などのシーンが考えられる．本論文の 6 章ではシナリオ 1 の環境での実験を示すが，シナリオ 2 と 3 については，携帯端末上で動作するモバイル WD を提案し，

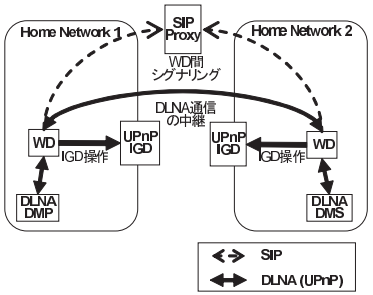

図 2　2 つのホームネットワーク間の接続
Fig. 2　Connection between two home networks.

実装と実験を行っている[11]．

これらの設計方針とシナリオを実現する DLNA 情報家電向け宅外接続支援機構を次節以降に説明する．

4.3　提案システムの概要

図 2 に，WD を用いたホームネット間接続図を示す．WD は，それぞれ SIP UA として動作する機能を持つ．各 WD は，一意に割り当てられた SIP URI を使って，別のブロードキャストドメインに存在する WD と協調して動作する．SIP サーバ，SIP URI，接続先 WD（5.1 節で述べるフレンドリスト）の情報は，あらかじめ WD に設定されていると仮定する．WD は，SIP 網を経由して接続先 WD から DLNA 機器の状況を把握するとともに，ユーザに接続先情報を提供する．

ユーザは，WD に対して接続先 WD の選択，接続先の DLNA 機器の選択，接続開始，接続停止などを指示する．これにより，インターネットを隔てた遠隔の DLNA 機器に対して，擬似的に同一ドメインに存在する機器に対して操作するのと同じ操作環境を提供する．

4.3.1　システム構成

WD を実装する機器は，各ホームネットワークに 1 つ配置すればよい．WD の実行環境としては，ホームサーバのほか，それよりプロセッサ性能やメモリ容量の制約の強いセットトップボックスなどに実装することも考えている．前節で述べたとおり，WD は SIP UA として動作し，WD 間の通信は SIP サーバを経由して行う．また，WD は NAT 透過に対して UPnP IGD（Internet Gateway Device）[12] を利用する．具体的には，IGD の検出，IGD に割り当てられたグローバル IP アドレスの取得，IGD の持つ NAT テーブルへのポー

トマップの追加と削除などを行う．これらの操作は，WD が UPnP CP（Control Point）として動作し，UPnP IGD に用意された WANIPConnection サービスをリクエストすることで実現する．ポートマップは，以下の各節で述べる SIP メッセージ（SSDP 相当機能など），UPnP Proxy 間の中継メッセージ（SOAP，GENA，デバイス記述ファイルのダウンロードなど），HTTP Proxy によるコンテンツ転送，の 3 種類を作成する．なお，UPnP IGD は一般的な家庭向け NAT ルータに実装されている．

このほか，WD からユーザインタフェースを分離する目的で，WD コントロールポイント（WDCP）を設置することもできる．このとき，WD は UPnP Device として振る舞い，WDCP は UPnP CP として実装する．WDCP は，DMC と統合して実装してもよい[13]．ユーザは，遠隔接続を開始する際 SIP URI を指定する必要がある．これは，ENUM などを利用することによって電話番号の入力程度の複雑さに抑えることができる．

4.3.2　SIP メッセージによる RPC

WD は，SIP を用いて通信先 WD の IP アドレスを取得する．遠隔の WD と協調した動作を行うにあたり，SIP の MESSAGE メソッドを利用した RPC（Remote Procedure Call）によるメッセージパッシングを利用する．すなわち，宛先の WD と対応する SIP URI を To ヘッダ，送信元 WD の SIP URI を From ヘッダに設定し，BODY 部分に XML で成形された RPC メッセージを挿入する．RPC 応答は，SIP MESSAGE メソッドの応答として，200 OK とともに戻り，変数名をタグの名前として，その値を囲んだ要素を配置する．戻り値は 0 個から複数個設定できる．

なお，WD の名前解決や RPC は，SIP 以外にも XMPP[14] などのプロトコルを用いることでも実現できると考えられる．我々が SIP を用いたのは，SIP が XMPP よりも IP 電話端末との連携に便利であること，HTTP と相性が良いことなどの理由による．

4.3.3　機器検出情報の転送

WD は，DLNA の SSDP 通信に相当する機器検出情報を SIP による RPC を用いて転送する．具体的には，WD が SSDP によって同じドメインにある機器を検出し，その情報を RootDeviceSummary.xml にまとめる（**図 3** ①〜②）．その後，SIP を通して RootDeviceSummary 情報の要求を受けたときに返答する（図 3 ③）．**図 4** に RootDeviceSummary.xml の例を示す．このファイルは，各 DLNA 機器のデバイス記述ファイルから，それぞれ UDN（Unique Device Name），friendlyName，および deviceType を抽出してまとめたものである．ユーザは，この機器一覧情報の中から接続を行う機器を選択し，機器の共有を開始する．このとき，WD は共有する遠隔 DLNA 機器のデバイス記述情報を模倣する UPnP Proxy プロセスを生成する．このプロセスは，UPnP CP に対して SSDP，SOAP，GENA のサービスを本来の DLNA 機器に代わって提供する（図 3 ④）．

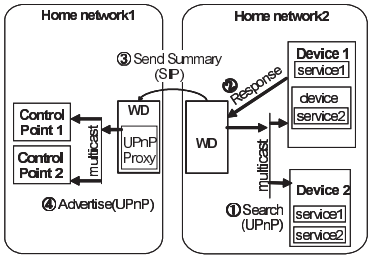

図 3　DLNA 機器情報の転送
Fig. 3　Transmission of DLNA device information.

```
<root xmlns="urn:wormhole-device:RootDeviceSummary-1-0">
 <rootDeviceList>
  <rootDevice>
   <UDN>635526b4-ff94-4ceb-b855-06654098b0e6</UDN>
   <friendlyName> Media Server1 </friendlyName>
   <deviceType>urn:schemas-upnp-org:device:MediaServer:1
  </rootDevice>
  <rootDevice>
   <UDN>635526b4-ff94-4ceb-b855-6846874657ef4</UDN>
   <friendlyName> Media Server2 </friendlyName>
   <deviceType>urn:schemas-upnp-org:device:MediaServer:1
  </rootDevice>
 </rootDeviceList>
</root>
```

図 4　RootDeviceSummary.xml の例
Fig. 4　An example of RootDeviceSummary.xml.

このように，同じドメインの機器情報を要約して送信することで，遠隔ユーザに公開する機器の取捨選択（アクセス制御）も可能となる．アクセス制御については，5 章で述べる．

4.3.4　UPnP Proxy

図 5 に，UPnP 通信中継プロセス UPnP Proxy の概略を示す．UPnP Proxy プロセスは，ターゲットとなる DMS のデバイス記述情報をダウンロードし，ターゲットと同じ UPnP Device サービスを提供する．DMP は，UPnP Proxy のデバイス記述情報をもとに，UPnP

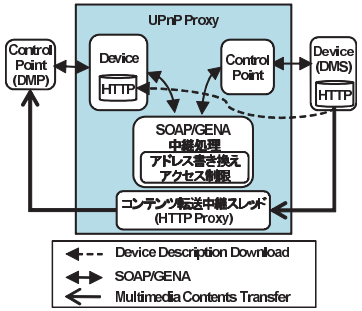

図 5　UPnP Proxy の動作
Fig. 5　Outline of a UPnP Proxy operation.

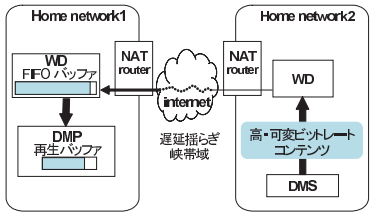

図 6　コンテンツバッファリングの模式図
Fig. 6　A diagram for contents buffering.

Proxy に対して GENA，SOAP 要求を送信する．UPnP Proxy は，内部に生成する UPnP CP によってこれをターゲットの DMS へ送信し，その応答を受信して DMP へ中継する．

UPnP Proxy は，中継メッセージを書き換える場合が 2 通りある．1 つは，SOAP，GENA のメッセージ中に DMS，DMR などのプライベート IP アドレスが含まれる場合である．2 つ目は 5 章で述べる DMS のコンテンツ一覧の一部を制限する機能（アクセス制御）によるものである．これらのアドレスやコンテンツ情報を書き換えることによって，目的とする通信とアクセス制御を実現する．コンテンツ転送の中継については，次項で説明する．

4.3.5　コンテンツ転送のバッファリング

一般に LAN を用いるホームネットワーク内の接続に比べて，ADSL などを経由するインターネット回線の方がスループットが低い．また，回線の品質も安定しない．DLNA 機器は家庭内 LAN によるコンテンツ転送を想定しているため，インターネットを経由する通信遅延への対策が必要となる．UPnP Proxy は，図 5 に示すように HTTP Proxy と呼ぶスレッドによってコンテンツ転送を中継する．HTTP Proxy の役割は，インターネットを経由するストリーム遅延の揺らぎを解消し，DMP の再生品質を向上させることである．DMP から DMS へコンテンツ一覧を取得する SOAP アクション “Browse” が発行され，その結果を WD が中継するときに HTTP Proxy を起動する．HTTP Proxy は，DMP 内部の再生バッファに対して十分に大きい容量のバッファを有し，コンテンツを蓄積してから DMP に送り出す（**図 6**）．

5.　アクセス制御

WD は，DLNA 機器を自動的に宅外に公開する．したがって，安全のためにアクセス制限機能を設ける必要がある．我々は，接続対象ユーザごとに公開する機器やコンテンツを制限する機能を導入した．また，UPnP Proxy を介する GENA，SOAP とコンテンツ転送パケットに対する IPsec 暗号化をサポートした．WD は，SIP を用いた RPC によって接続先 WD と IP アドレスを交換した後，Racoon2 [15] を起動して IKE（Internet Key Exchange）v2 による鍵交換と ESP（Encapsulating Security Payload）プロトコルを用いたパケットの暗号化を実現する．また，接続先家庭内の DLNA 機器とプライベートアドレスが衝突する場合，仮想的なアドレスを割り当てて通信ができるようにする．

5.1　フレンドリストによる制限

各 WD が一意な SIP URI を持つことはすでに述べた．これらの SIP URI は，SIP メッセージが SIP サーバを通過するたびに SIP Proxy 認証を受ける．さらに，ユーザは接続を許可する遠隔 WD の SIP URI を，自身の WD に登録する．この接続を許可する SIP URI のリストをフレンドリストと呼ぶ．WD は，これに記載される以外の SIP URI を持つ WD からの接続を拒否する．また，個々の WD は SIP サーバを通過しないメッセージを破棄する．

5.2　ルール設定による機器一覧制限

WD は，Root Device Summary を用いた SSDP に相当する機能を提供する．この情報を交換する際に，あらかじめ設定されたルールによって，相手に渡す DLNA 機器の情報を制限することができる．公開を制限する DLNA 機器は，UPnP の Device Type または UDN でルール設定する．たとえば，宅内のすべての DMR は宅外に公開しない，またはリビングの DMS だけ公開する，などの指定ができる．また，接続先の WD の SIP URI によって適用範囲を変えることができる．図 6 に示すように，フレンドリスト中の特定のメンバ（祖父母宅）のみに公開する，といった設定ができる．

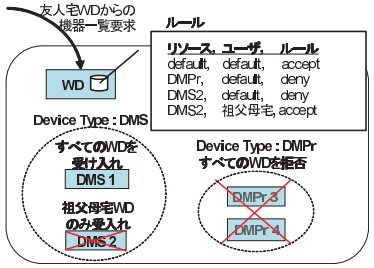

図 7　ルール設定による機器一覧アクセス制限の例
Fig. 7　An example of rule-based access control.

また，すべての SIP URI に対して適用されるデフォルトの値をあらかじめ設定しておく．これにより，ユーザがルール設定をまったく行わなくても，宅外から利用する可能性の少ない機器に対して安全な運用を図る．たとえば，外部からアクセスする需要が少ない DLNA 対応プリンタ DMPr をあらかじめアクセスできないようにしておく，などの設定が可能である（**図 7**）．ルールは XML で記述し，これらは GUI によって以下の項目を選択的に指定すればよい．ルールに記述できる項目は以下のとおりである．

- 家庭内の全 DLNA 機器に対する公開または非公開のデフォルト値
- 同一のデバイスタイプを有する家庭内の DLNA 機器群に対する公開または非公開のデフォルト値
- 個別の DLNA 機器が有する全サービスとコンテンツに対する公開または非公開のデフォルト値
- 個別の DLNA 機器が有する各サービスとコンテンツに対する公開または非公開の情報
- 公開するユーザを限定するための SIP URI

図 8 に，アクセス制御用 XML の例を示す．図中 2 行目は，家庭内の全 DLNA 機器をフレンドリストに記載されたユーザにデフォルトで公開する場合の記述である．次の 3 行は，Device Type が MediaServer（DMS）の機器公開を意味する（図 7 の DMS1 公開）．それに続く device タグ部分の 6 行は，記述された uuid を持つ DMS を SIP URI:user2@sipserver.uec.ac.jp のユーザのみに公開することを指定する（図 7 で，祖父母宅 WD のみに DMS2 公開に相当）．また，下 5 行部分は Printer をいずれの遠隔ユーザにも公開しないことを示す．

5.3　ルール設定によるコンテンツ一覧制限

機器一覧と同様に，DMS の中のコンテンツについても一覧の制限を行うことができる．

```
<resources>
  <rule user="">accept</rule>

  <deviceType id=
      "urn:schemas-upnp-org:device:MediaServer:1">
    <rule user="">accept</rule>
    <device id=
      "uuid:000000000000-0000-0000-000000-000002">
      <rule user="">deny</rule>
      <rule user="user2@sipserver.uec.ac.jp">
       accept</rule>
    </device>
      <container id ="0">
        <rule user="">deny</rule>
        <container id ="000003">
          <rule user="">accept</rule>
        </container>
      </container>
  </deviceType>

  <deviceType id=
      "urn:schemas-upnp-org:device:Printer:1">
    <rule user="">deny</rule>
  </deviceType>
</resources>
```

図 8　アクセス制御用 XML の例
Fig. 8　An XML example for access control.

コンテンツ一覧情報を含む UPnP 通信は，WD 間で中継される．WD は，この通信に認証ヘッダを添付することで通信相手となる WD の識別と認証を行う．以下に，**図 9** の動作手順を説明する．

(1)　DMP 側 WD が，DMS 側の WD に対して GetTicket 要求を SIP RPC 経由で行う．これは，アクセス権とそれに対応したパスワードの発行を求めるものである．
(2)　要求を受けた DMS 側 WD は，有効期限付きのパスワードを発行する．このときパスワード文字列は直接送信せず，Diffie-Hellman 鍵共有[16] を用いる．
(3)　DMP 側 WD は，DH 鍵共有によって得た鍵を SH1 1 方向ハッシュ関数で変換し，認証情報として SOAP 要求のヘッダに添付する．
(4)　DMS 側の WD は，認証情報が正しいことが確認できた場合にのみ，DMS へ SOAP

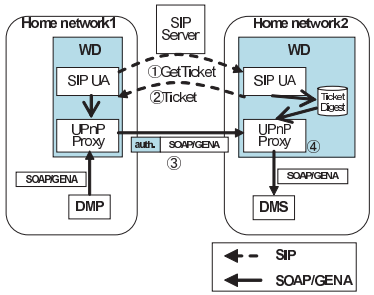

図 9　UPnP 通信の識別と認証
Fig. 9　Identification and authentication of UPnP communication.

要求を中継する．さらに，その応答を DMP 側の WD に中継する．その際コンテンツ一覧に含まれるフォルダに相当するコンテナ，ファイルに相当するアイテムの情報についてルールと照合を行う．

以上により，WD が通信を中継するか否かを判断する．ルールの記述方法は次に述べるように 2 種類あり，それぞれ異なる動作を行う．また，対象とする SIP URI ごとに異なる種類のルールを設定し併用することもできる．

5.3.1　Accept-based ルールによる運用

基本的にコンテンツ情報の中継を許可し，ルールで指定した特定のアイテム，コンテナに関する情報を削除するルールである．**図 10** に例を示す．ある SIP-URI“A” を持つ WD に対して，映画コンテナの要素を削除するルールを設定する．このとき，SIP-URI“A” 以外のフレンドリスト・メンバに対しては，図 10 の上側に示すコンテナ一覧を返答する．ただし，SIP-URI“A” を持つ WD からコンテンツ一覧要求があった場合，図 10 の下側に示す制限されたコンテナ一覧を返答する．映画コンテナ以下にあるアイテムも再帰的に検索・拒否登録されるため，ショートカットによって他のコンテナから映画コンテナが参照されることもない．

5.3.2　Deny-based ルールによる運用

基本的にコンテンツ情報の中継を不許可とし，許可されたものをコンテナ階層の最上位に提供する方法である．これによってコンテンツファイル一覧のツリーの構造を変更する．**図 11** に例を示す．ある SIP-URI“B” が持つ WD からルートコンテナへのコンテンツ一覧要求があった場合，その SIP-URI“B” に対して中継が許可されている映画コンテナの要素

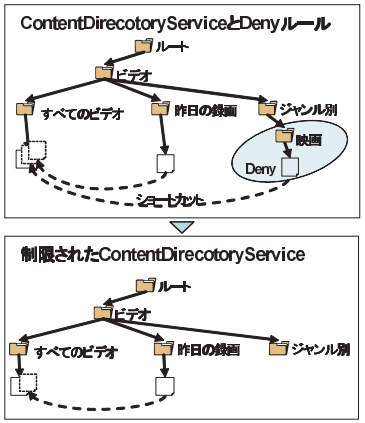

図 10　Accept-Based ルールによるコンテンツ一覧制限
Fig. 10　Contents list limitation by Accept-Based rules.

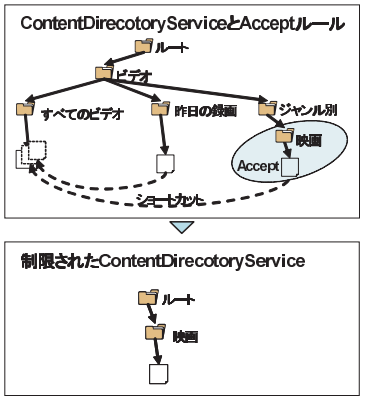

図 11　Deny-Based ルールによるコンテンツ一覧制限
Fig. 11　Contents list limitation by Deny-Based rules.

だけを提供する．このとき，ルートコンテナ以外への要求についてはその応答を書き換えることはない．図 8 中ほどの container タグ部分に，container id =”000003”のみ公開する例を示す．

6. 実装と評価

一般家庭のホームネットワーク環境を模した環境を実際に構築し，DLNA 機器の家庭間接続の実証実験を行った．また，WD がアクセス制御を行う際の評価としてコンテンツ一覧取得にかかる時間を測定した．さらに，コンテンツ再生時のスループットを測定した．なお，本章に述べる WD 間の通信（表 3 の直接通信を除く）では 5 章冒頭に述べたように IPsec 暗号化を用いている．

6.1 実　　装

表 1 に，WD プロトタイプの実行環境と実装について示す．WD は，NIC を 1 つ持つ標準的な PC および NAS（ともに Linux）に C 言語で実装した．UPnP，SIP などのライブラリにはオープンソースのものを利用した．なお，4.2 節で述べたシナリオ 3 を実現する WD の携帯端末上での実装については文献 11) を参照されたい．

6.2 評　　価

4 つのホームネットワーク環境を構築し，それぞれ WD を実行する PC または NAS（Network Attached Storage）と市販の DLNA 機器を配置した．各ホームネットワークには，インターネットサービスプロバイダが提供する FTTH，CATV，ADSL などの家庭向けインターネット接続サービスを用いた．また，必要に応じて市販の家庭用 NAT ルータを導入した．SIP サーバは，4 つのホームネットワークとは別にグローバルネットワーク上に配置した．**図 12** に，実験に用いた 2 つのホームネットワークの構成を示す．

表 1　WD プログラムの実行環境と実装
Table 1　Execution environment and implementation of the WD program.

Item		Environment
PC	CPU	PentiumD 3 GHz
	RAM	1 GB
	NIC	1000BaseT
NAS	CPU	PowerPC 266 MHz
	RAM	128 MB
	NIC	1000BaseT
OS		FedraCore 6 Linux
Language		C
Library		Portable UPnP Library 1.4.6 The GNU oSIP Library 2.2.2 The eXtend oSIP Library 2.2.3
Source code		Approximately 12,100 lines

各ホームネットワークの DMP 側 WD から DMS 側 WD への接続を試みた．そして，DMP から遠隔ホームネットワークにある DMS のコンテンツ一覧を取得し，コンテンツを再生することができた．これにより，WD が設計方針を満たす DLNA 機器の宅外遠隔接続のための支援機構として動作することを確認した．

6.2.1 WD による通信中継処理のオーバヘッド

DMP が DMS のコンテンツ一覧を取得する場合について，アクセス制御する場合としない場合の応答時間を測定した．**表 2** に，測定環境を示す．アクセス制御を行う場合，DMS（DiXiM）上に 100 個のアイテムを置き，Accept-based および Deny-based ルール設定により 10 から 90 アイテムを中継する場合の応答時間を DMP 側の C プログラムで測定した．アクセス制御を行わない場合については，DMS 上に置くアイテム数を 10〜90 とし，その一覧取得の応答時間を測定した．

図 13 に，DMS 側 WD を PC（表 1 参照）で実行したときの結果を示す．いずれの場合

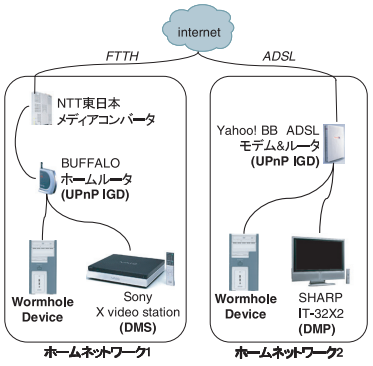

図 12　実験に用いたホームネットワーク
Fig. 12　Experimental home networks.

表 2　DMP-DMS 間通信実験の環境
Table 2　Experimental environment for communication between DMP and DMS.

DMP side	WD on PC 測定用自作 C プログラム Internet: KDDI 光 One
DMS side	WD on PC or NAS DiXiM2 Ver.2.4.10 on Windows PC Internet: NTT B フレッツ

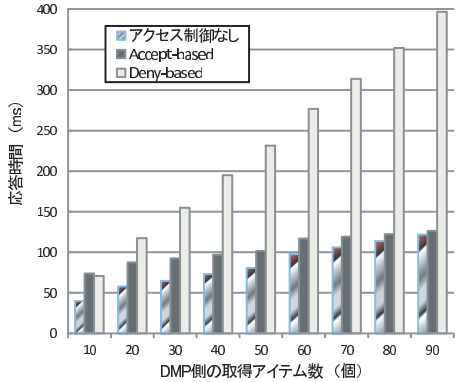

図 13　コンテンツ一覧取得の応答時間（DMS 側 WD：PC）
Fig. 13　Response time to get a directory of contents, when we execute WD on a PC for DMS side.

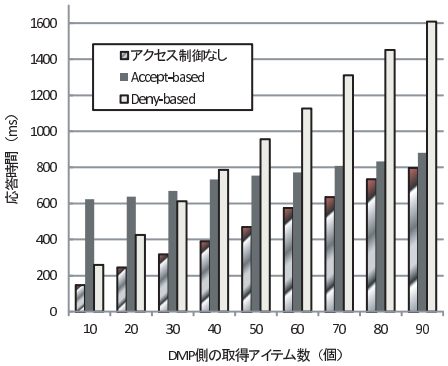

図 14　コンテンツ一覧取得の応答時間（DMS 側 WD：NAS）
Fig. 14　Response time to get a directory of contents, when we execute WD on a NAS for DMS side.

も，DMP 側で取得するアイテム数が増加すると応答時間が増加する．これは，通信データ量が増加するためである．アクセス制御なしの場合に比べてアクセス制御時の応答時間が長くなるのは，設定されたルールに基づいて中継を許可するアイテムを選別する処理を行うためである．したがって，アクセス制御なしとありとの差分がルール処理時間を表す．アクセス制御処理のオーバヘッド（アクセス制御なしとありとの差分）は，ルール数に応じて増加する．この理由は，WD がコンテンツ一覧を XML パーサを通してメモリ上に DOM（Document Object Model）ツリーとして展開し，各要素がルールに適合しているかどうかを検査するためである．

Accept-based ルールではデフォルトをアクセス許可（Accept）とし，アクセスを拒否するアイテムに対してルールを列挙する．そして，（100-ルール数）のアイテムを DMP に中継する．図 13 では，横軸に DMP が取得するアイテム数を表しており，その数が多いほど Accept-based ルールが少ない場合を表す．したがって，アクセス制御なしと Accept-based の応答時間グラフの差は横軸の値が小さい（ルール数が多い）ほど大きい．図 13 から，Accept-based ルール処理に約 0.4 ms/ルールかかることが読み取れる．

Deny-based ルールではデフォルトをアクセス拒否（Deny）とし，アクセスを許可するアイテムに対するルールを列挙する．したがって，DMP が取得するアイテム数が多くなるほどアクセス制御なしとの差分も大きくなる．図 13 から，Deny-based ルール処理時間は約 3 ms/ルールであることが分かる．この値は，Accept-based ルール処理時間よりも大きい．この理由は，Deny-based ルール処理によるコンテンツ一覧ツリーの再構築が，Accept-based ルールによってコンテンツ一覧ツリーから禁止されたアイテムを削除する処理よりも複雑であることによる（図 10 と図 11 参照）．なお，IPsec 暗号化の有無による応答時間の増加は 10 ms 未満であった．

図 14 に，DMS 側 WD を NAS（表 1 参照）で実行したときの結果を示す．DMP 側で取得するアイテム数が増加すると応答時間が増加する傾向は，図 13 と同様である．ただし，図 14 の応答時間はいずれも図 13 に比べて長くなっている．WD が UPnP 通信を中継する場合，送信側 WD でメッセージに認証ヘッダを付与し，受信側 WD で認証と認証ヘッダの除去などの処理を行う．そのため，応答時間が WD を実行する計算機性能の影響を受ける．アクセス制御のルール処理は DMS 側 WD で実行されるが，その実行環境を NAS に変えると，Accept-based ルール処理に 5 ms から 8 ms/ルール，Deny-based ルール処理に 9 ms から 11 ms/ルールとなった．

DMP は，取得したコンテンツ一覧を画面に表示し，カーソルによって選択させるインタフェースを提供する．このため，100 アイテムより多いアイテムを取得することは稀である．以上から，WD の中継による UPnP 通信の遅延は WD の実行環境の性能に依存するものの，今回の実験では SOAP の典型的なタイムアウトである 30 s に比べて十分小さな値であった．

6.2.2　コンテンツ通信の中継性能

WD は，DMS と DMP の間のコンテンツ通信の中継を行う．この通信性能と安定性につ

表 3　中継方式によるスループットの比較（Kbps）
Table 3　Comparison of throughput with and without relay by WD (Kbps).

DMS side	DMP side		
FTTH1	FTTH2	ADSL	CATV
direct transfer	54,250.3	8,934.8	19,716.3
via WD	58,313.8	8,096.4	19,163.8

いて考察する．**表 3** は，コンテンツ通信を WD が中継する場合と，WD なしに DMS と DMP が直接通信する場合のスループットを示す（10 MB の同一コンテンツ転送 30 回の平均）．測定されたスループットは，インターネット回線の違いとその回線の状態の影響を大きく受ける．回線の状態が安定している場合，WD を経由することによるスループットの低下はほとんど観測されなかった．同一回線でスループット値に差が出た理由は，主にインターネット回線の混雑状態による．

次に可変ビットレートの動画コンテンツをストリーミング再生した場合を想定して，DMP には単位時間あたりの流量が一定でない HTTP-GET の取得パターンを要求させた．さらに，通信に遅延が生じた場合に DMP の再生が受ける影響を測定するため，DMP 内のコンテンツ再生のためのバッファ使用量を測定した．測定に際しては，DMS 側に CATV，DMP 側に ADSL 回線を用いた．この間の平均転送スループットは 1,578.3 Kbps であった．また VBR コンテンツの平均ビットレートは 1,575.2 Kbps である．DMP 内の再生バッファ容量は最大 1 MB とした．

図 15 に，HTTP Proxy の FIFO バッファを使わない場合の DMP の再生スループット（DMP 内のバッファからコンテンツを出力するスループット）と DMP 内の再生バッファ使用量を示す．DMP 側では，再生指示から 4 秒後に再生を開始する．しかし VBR コンテンツのビットレート揺らぎ，インターネットの遅延揺らぎにより，徐々に DMP 内の再生バッファ使用量が減り，最終的に再生の途中でバッファが枯渇した．これに対して，**図 16** に HTTP Proxy 内 FIFO バッファを 10 MB 使用した場合を示す．このとき，DMP 側では再生指示から再生までは 17 秒遅れるが，DMP 内再生バッファの不足分が短時間で HTTP Proxy の FIFO バッファから供給される．結果的に，DMP 内の再生バッファは枯渇せず，安定した再生を続けることができた．

DMS-DMP 側 WD 間の通信経路がインターネットを経由する場合，通信経路の状態によって通信スループットが突発的に低下することがある．HTTP Proxy 内の FIFO バッファ容量やビットレートの異なるコンテンツに対して遠隔通信と再生の実験をしたところ，以下

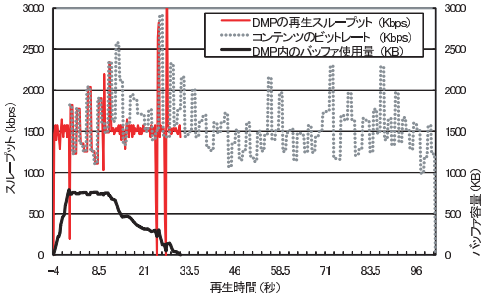

図 15　中継バッファなしのコンテンツ中継
Fig. 15　Contents relay without relay buffer.

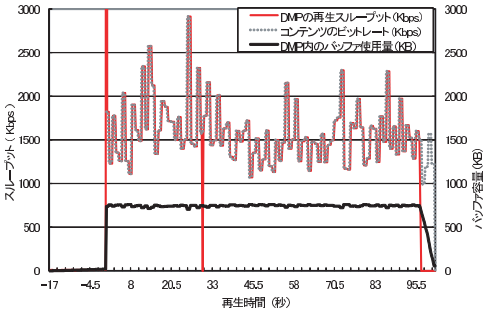

図 16　中継バッファを利用したコンテンツ中継
Fig. 16　Contents relay with buffering.

のことが分かった．

（1）　HTTP Proxy 内の FIFO バッファが有効に働く条件は，DMP によるコンテンツ再生スループットが一時的に DMS-DMP 側 WD 間の通信スループットを超える場合，かつ再生に必要なコンテンツデータを HTTP Proxy 内の FIFO バッファから供給できる場合である．

（2）　DMS-DMP 側 WD 間の平均通信スループットを下回るか，それに近い値の再生スループットを必要とするコンテンツに対しては，HTTP Proxy 内の FIFO バッファ容量を増やすほど，一時的な通信スループット低下への耐性が高くなり再生停止回数を減らすことができる[11]．

(3) DMS-DMP 側 WD 間の平均通信スループットに対して再生スループットが低く，DMP 内の再生バッファが枯渇しないコンテンツに対しては必ずしも HTTP Proxy 内に大きな FIFO バッファを設ける必要はない．逆に，HTTP Proxy 内の FIFO バッファが枯渇するほど再生スループットに対して通信スループットが不足する場合は，コンテンツ再生が停止してしまう．

7. おわりに

本論文では，既存の DLNA 機器を宅外から利用するために開発した WD について述べた．WD は，DLNA 機器の遠隔接続に必要なネットワークの設定，通信相手の認証，DLNA 機器のホームネットワーク間での共有とそれらのアクセス制御機能を提供する．WD の特徴は，既存の DLNA 機器や NAT ルータに変更を加えることなくホームネットワークに導入することができる点である．

市販の DLNA 機器や NAT ルータ，家庭向けインターネット接続サービスを使った環境を構築して相互接続実験を行った．その結果，操作の遅延が十分少なく設定・操作が簡単なアクセス制御を実現できることを確認した．今後の課題としては，著作権保護のためのリンクプロテクションへの対応などがあげられる．

謝辞　実験に協力してくれた電通大院生の小山卓視君に感謝します．なお，本研究の一部は，電気通信大学と船井電機（株）の情報家電に関する共同研究（FUN-X プロジェクト）の援助による．

参考文献

1) Digital Living Network Alliance: DLNA Networked Device Interoperability Guidelines expanded October 2006, Digital Living Network Alliance (2006).
2) Srisuresh, P., Jasmine Networks and Egevang, K.: Traditional IP Network Address Translator (Traditional NAT), RFC 3022 (2001).
3) 武藤大悟, 吉永　努：ワームホールデバイス：DLNA 情報家電の遠隔相互接続支援機構, マルチメディア，分散，協調とモバイル（DICOMO2007）シンポジウム，pp.134–138 (2007).
4) DLNA. http://wwwDLNA.org/
5) UPnP Forum: UPnP Device Architecture 1.0 Version 1.0.1, UPnP Forum (2003).
6) Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler E.: SIP: Session Initiation Protocol, RFC 3261 (2002).
7) Nakamoto, T. and Kuri, N.: Siphnos – Redesigning a Home Networking System with SIP, *Proc. 6th IEEE International Conference on Computer and Information Technology* (2006).
8) Oh, Y.-J., Lee, H.-K., Kim, J.-K., Paik, E.-H. and Park, K.-R.: The DLNA Proxy System Architecture for Sharing In-Home Media Contents via Internet, *Proc. 8th International Conference on Advanced Communication Technology*, pp.1855–1858 (2006).
9) 茂木信二，田坂和之，テープウィロージャナポンニワット，堀内浩規：情報家電の広域 DLNA 通信方式の提案，信学技報 NS2007-13, Vol.107, No.6, pp.71–76 (2007).
10) Oh, Y.-J., Lee, H.-K., Kim, J.-K., Paik, E.-H. and Park, K.-R.: Design of an Extended Architecture for Sharing DLNA Compliant Home Media for Outside the Home, *IEEE Trans. Consumer Electronics*, Vol.53, pp.542–547 (2007).
11) 小山卓視，武藤大悟，呉　敬源，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，情報処理学会ユビキタスコンピューティングシステム研究会報告，Vol.2008, No.18, pp.1–8 (2008).
12) UPnP Forum: InternetGatewayDevice: 1, ver.1.0, UPnP Forum (2001).
13) Wu, J.Y., Yosinaga, T., Muto, D. and Koyama, T.: Mechanism for Sharing Media Content in Multiple Home Network Environments, IPSJ Technical Report, 2008-UBI-19 (2008).
14) Saint-Andre, P. (Ed.): Extensible Messaging and Presence Protocol (XMPP) Core, RFC 3920 (2004).
15) The Racoon2 project. http://www.racoon2.wide.ad.jp
16) Rescorla, E.: Diffie-Hellman Key Agreement Method, RFC 2631 (1999).

(平成 20 年 3 月 13 日受付)
(平成 20 年 9 月 10 日採録)

武藤　大悟（学生会員）

昭和 58 年生．平成 18 年武蔵工業大学工学部システム情報工学科卒業．平成 20 年電気通信大学大学院情報システム学研究科博士前期課程修了．ホームネットワーク等に興味を持つ．現在，KDDI に勤務．

吉永　　努（正会員）

昭和 38 年生．昭和 61 年宇都宮大学工学部情報工学科卒業．昭和 63 年同大学大学院工学研究科修士課程了．同年より宇都宮大学工学部助手．平成 9 年から翌年にかけて電子技術総合研究所・客員研究員．平成 12 年より電気通信大大学院情報システム学研究科・助教授．現在，同准教授．博士（工学）．並列計算機アーキテクチャ，クラスタ計算，ホームネットワーク等に興味を持つ．IEEE，電子情報通信学会各会員．