

# 情報家電ネットワークの遠隔相互接続のための ネットワークアーキテクチャ

武藤 大悟<sup>†</sup> 吉永 努<sup>†</sup>

電気通信大学 大学院情報システム学研究科<sup>†</sup>

## 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<sup>[1]</sup>に準拠した機器はその相互接続性の良さから、HD レコーダや大型テレビ等の AV 機器を中心に数を増やしつつある。一方で家庭内に閉じている情報家電ネットワークを家庭の外へ拡張し、外部または異なる家庭間で相互に接続・操作を行うことは、一般家庭でのインターネット接続環境の広帯域・常時接続化もあいまって、アプリケーションの応用可能性を大きく広げることが期待される。本稿では DLNA ガイドラインの中核をなす UPnP スタック<sup>[2]</sup>を実装した機器を異なるドメイン間で相互に接続する機構を提案する。これにより既存の情報家電ネットワークに参加する機器を再編成せずとも、それらの機器からインターネット越しに遠隔相互接続を利用することが実現する。以降、それらを実現するための相互接続網の構成とその通信方法を示す。

## 2. 相互接続網とその要素

異なるドメイン間で UPnP 機器を接続するためにはネットワーク上の位置解決問題や後述する NAT 透過に関する問題を解決する必要がある。ホームネットワークではその特性からユーザーからの設定支援がごく簡単なものに限られるため、それらを半自動的に解決するために図 1 に示すような相互接続網を構成する。扱う内容に応じて異なる 2 つの経路、シグナリングチャンネルとデータチャンネルを設定する。データチャンネルは各 UPnP 機器が直接的に通信を行うために利用され、その接続の状態は SIP で構成されたシグナリングチャンネルによって開始・停止などの制御を受ける。相互接続網を構成する各要素を図 1 に示し以下をその説明とする。

### Wormhole Device(WD)

このデバイスは UPnP スタックと SIP スタックを扱う。UPnP スタック上では後述する UPnP IGD

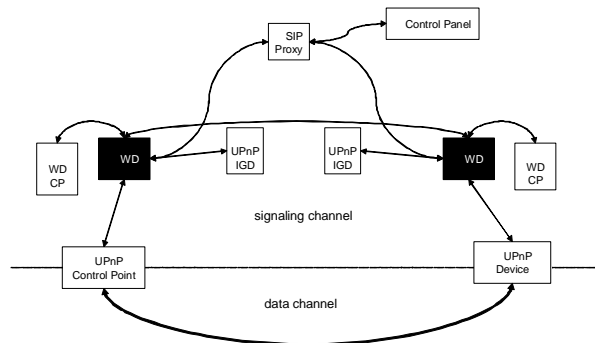


図 1 網構成要素と各要素間の通信

の Control Point(CP)として振舞うほか、WD には Device として操作される。また、SIP スタック上では SIP Proxy を利用する User Agent(UA)として動作する。

### UPnP Control Point と UPnP Device

一般的な UPnP 機器でありここでは DLNA 基準の機器を想定している。

### Wormhole Device Control Point (WDCP)

UPnP デバイスである WD を操作する CP である。ユーザーが WD を操作して、異なるドメインの UPnP 機器へ接続する場合、また、自ドメイン機器が呼び出しを受けた際の接続の認否に関する設定を行う場合に利用する。

### SIP Proxy

UA として WD と、後述の Control Panel を持つ SIP Proxy サーバーである。SIP の REGISTER リクエストによってこのサーバーに登録された UA の間で交わされる SIP リクエストを中継する。登録する UA は digest 認証方式を用いて認証を通過しなければならないものとする。こうすることにより、中継される SIP リクエストの発信者の身元に一定の信頼性が確保される<sup>[3]</sup>。

### Control Panel

網構成にかかわる情報を管理する役割を持つ SIP UA である。たとえば複数の WD がコンテンツの共有を行う際、参加する WD をグループとして管理するとき、これの持つ SIP UID とグループの対応付けする情報が利用される。

### UPnP IGD

現状の家庭向けインターネット接続で多く導入

“A network Architecture for remote communication between digital appliances”

<sup>†</sup> Daigo Muto and Tsutomu Yoshinaga  
Graduate School of Information Systems, the University of Electro-Communications

されている，IPv4 下の 1 対多型 Network Address Translation(NAT)環境下では，個々の機器に外部から接続しようとした場合，いわゆる NAT 透過のために何らかの施策が必要となる<sup>[4]</sup>．本研究ではこの問題に対し，すでに広く一般家庭に普及している UPnP 対応 NAT ルータ (UPnP IGD)<sup>[5]</sup>を利用する．WD はこれを用いて WD 自身を外部ネットワーク向けサービスとして，または網からの要求に応じて各機器へのデータチャンネルを開くのに必要なポートマッピング等の動作を UPnP を通じて設定する．

### 3. 各要素間の通信

#### 3.1. WD 間の通信

相互接続の両端のドメインに存在する WD の通信は網上の Proxy を中継して行われる．Proxy に登録された WD は SIP UID によって一意に識別される．WD はシグナリングを行う際に SIP の MESSAGE メソッドを利用したリクエスト<sup>[6]</sup>を UID を指定して網へ送信する．リクエストの message body には XML に整形された RPC(Remote Procedure Call)メッセージを挿入し，これを受け取った受信側の WD は message body に RPC に対する戻り値，エラーコード，エラーメッセージを XML に整形された形で挿入した MESSAGE リクエストへの"200 OK"の応答を返信する．

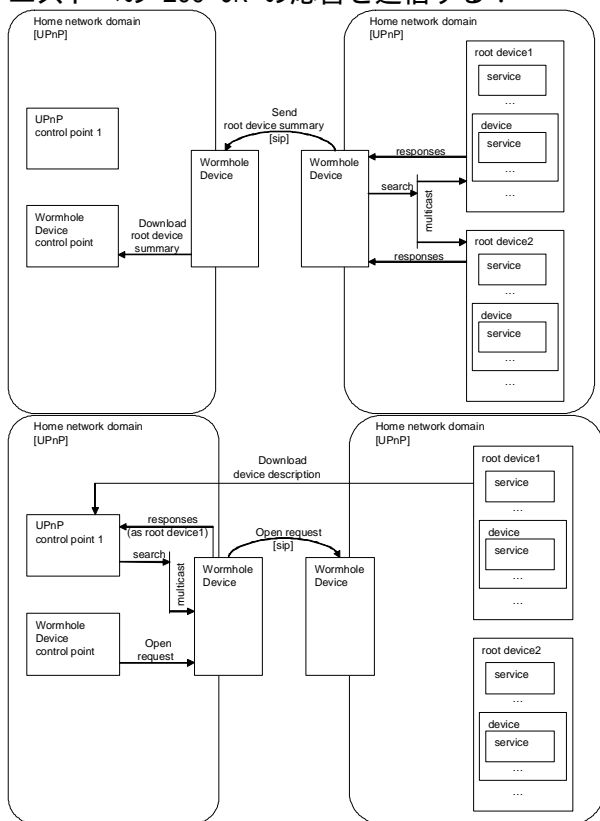


図 2 異なるドメインの UPnP device 検出

#### 3.2. 異なるドメインの UPnP 機器の検出

通常 UPnP CP は同じドメインの UPnP Device を検出するために SSDP を用いるが SSDP は同じドメイン内に限って有効であり異なるドメイン間にこの処理を拡張しようとした場合これを適切に中継することが必要となる．これに対して WD は以下の流れに示す方法を使って解決する．まず，それぞれのドメインの WD は同じドメイン内の Device を SSDP によって検出する(図 2 中 ~ )．WD は検出したこれら同一ドメインにある機器についての要約を作成し，通信先の WD と交換する(図 2 中 )．ユーザーが WDCP からの要約の中にある機器を公開することを選択すると WD は通信先 WD に指定された機器の公開を要求する(図 2 中 ~ )．また，WD は CP に対して，実際の公開先を実際の Device に代わって SSDP によって通知する．これにより，CP は本来の SSDP の処理に従いながら異なるドメインの Device に接続し，Device Description を取得し，SSDP による機器検出を終える．

ここまで述べた手法に従い実装を行った結果，それぞれの機能が期待された動作を行うことが確認できた．

### 4. おわりに

本稿では，主に SIP をシグナリング網として利用するユーザーによる複雑な設定動作を要求しない UPnP 機器の遠隔接続を実現するネットワークアーキテクチャを検討した．今後の課題としては，インターネットを経由する通信をより安全に行うための施策としての通信路の暗号化，WD 同士の接続や機器の共有する権限の管理を行う方法を盛り込んだ網構成の提案などが挙げられる．

**謝辞** 本研究の一部は，電気通信大学と船井電機㈱の情報家電に関する共同研究 (FUN X プロジェクト) の援助を受けて行われた．

#### 参考文献

- [1]DLNA, <http://www.dlna.org/en/consumer/home>.
- [2]UPnP Forum: "UPnP Device Architecture 1.0", Ver.1.0.1, p.73 (2003).
- [3]Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M. and E. Schooler, "SIP:Session Initiation Protocol", RFC 3261, (2002).
- [4]金森 重友,佐野 勝大,斉藤 允, 阪田 史:"SIP/UPnP 情報家電プロトコル"秀和システム p.286 (2005).
- [5]UPnP Forum: "InternetGatewayDevice:1", Ver.1.0, p.15 (2001).
- [6]J. Rosenberg, dynamicsoft, H. Schulzrinne, Columbia University, C. Huitema, D. Gurle, Microsoft Corporation "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC3428, (2002).