宅外機器の移動透過性を可能とする遠隔 DLNA 通信方式の提案

近藤千華

DLNA(Digital Living Network Alliance)準拠の情報家電が増加し始めている．しかし DLNA 準拠の情報家電は閉じたネットワークでしか利用することができないため，宅外からホームネットワーク内の DLNA 準拠の情報家電を利用するというニーズを満たすことができない．また，公衆無線 LAN が今後発達した際, 宅外の DLNA 準拠の情報家電を持ち移動しながらホームネットワーク内の情報家電を利用することも想定されるが，移動により IP アドレスが変わり通信が継続することができない問題が生じる．本稿ではそれらの問題を NAT-f(NAT free protocol)と Mobile PPC(Mobile Peer to Peer communication)を用いて解決する. 提案方式では DLNA 機器だけでなくホームネットワーク内にある機器すべてに利用することができる．

Proposal of Remote DLNA Communication System Realizing Mobility for Devices located on outside of Home

KONDO CHIKA

The number of DLNA-compliant products increase now. Because DLNA-compliant products are supported only in closed Network, user cannot satisfy to use DLNA-compliant products in the home network from outside. Also , when public wireless LAN developed in future, that I use an information household appliance in the home network while I have an information household appliance of DLNA conformity out of' house, and moving is assumed, but the problem that an IP address changes by movement, and communication cannot continue produces it. It solves those problems with NAT-f(NAT free protocol) and Mobile PPC(Mobile Peer to Peer communication) by this report. All machinery can use it not DLNA machinery by the suggestion method in home networks.

1. はじめに

近年デジタル情報家電が普及し始め，それらをネットワークで接続し利用するケースが増えている．中でも DLNA(Digital Living Network Alliance)[1]に準拠したデジタル情報家電は特に今後の普及が見込まれている．DLNA ではユーザがプレーヤ DMP(Digital Media Player)を利用するだけで，メディアコンテンツを保存している DMS(Digital Media Server)を自動的に発見し，利用することができる．DLNA 準拠のデジタル情報家電同士は，ネットワークを介してメーカの垣根を越えて利用することができる．DLNA に準拠したデバイスは, 2003 年に DLNA が発足してから 2009 年現在までに発売しているもので 1000 種弱, DLNA から認定を受けたもので 4000 種弱を数え，今後も増加することが見込まれる．

しかし，DLNA 準拠デバイスは，利用できる範囲が現在家庭内に限定されている．DLNA によって策定されたガイドラインでは家庭内のネットワークのみでのデジタル情報家電の利用を想定しており，屋外のネットワークから利用することができない．DLNA ではデバイス検出及びその制御に UPnP(Universal Plug and Play)との連携を想定しており，デバイス検出には SSDP(Simple Service Discovery Protocol)と呼ぶプロトコルを用いる．SSDP はマルチキャストを利用しているので宅外 DMP からインターネットを介して利用することはできない．また，グローバル IP アドレス空間にある DMP からホームネットワークのホームゲートウェイへアクセスを開始することができない．これは DLNA 機器を宅外から利用す

†名城大学理工学部情報工学科

る際に限ったことではなく一般に，NAT 越え問題と呼ばれている．さらに，同一セグメントにある DMP からのアクセス以外は DMS が無視する仕様となっており，宅外にある DMP が DMS のメディアコンテンツを利用できない．これらの課題に加え，将来移動通信が一般的になった場合，移動しながら DMS のメディア視聴が継続できないという課題がある．これは DMP の移動により IP アドレスが変化するためである．本稿ではこれらの課題を解決し，宅外にある移動機器から DLNA 準拠デバイスを遠隔操作することに加え，移動しながら DMS に保存されているメディアを継続して視聴を可能にする方式を提案する．

提案方式では NAT-f とその改造によりホームネットワークにある DMS を宅外 DMP から遠隔操作し，Mobile PPC を用いて DMP の移動通信継続を可能とする．

以下 2 章で DLNA の技術的課題と，既存技術による解決法を述べる．3 章で提案方式を述べ，4 章では既存技術との比較を行う．最後に 5 章でまとめを示す．

2. DLNA の技術的な課題と既存技術

2.1 DLNA の技術的課題

DLNA の策定したガイドラインでは各社製品が共通に対応すべきメディアフォーマット，情報家電の相互接続に用いる通信プロトコルやネットワークデバイスなどが規定されている．相互接続に用いる通信プロトコルとしてデバイスの検出や制御には UPnP, データ転送には HTTP がそれぞれ用いられる．ホームネットワーク内における DLNA のシーケンスを**図 1** に示す．

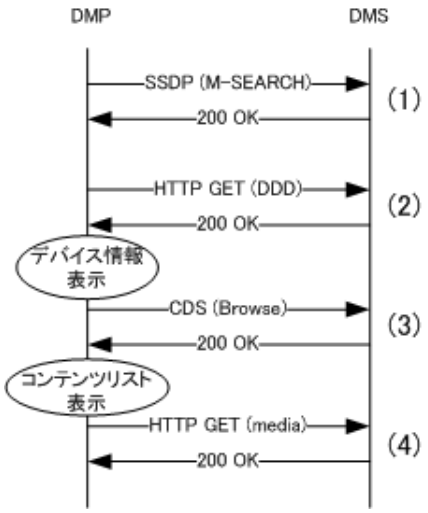

図 1　DLNA のシーケンス図

DLNA はこのシーケンスを経て DMP が DMS 発見し，DMS が保持するコンテンツを視聴する. 以下にその詳細を示す.

(1)　UPnP のプロトコルである SSDP の M-SEARCH メッセージを DMP から DMS へ送る．これはデバイスを検出するために用いられ，マルチキャストで送信される．このメッセージを受信した DMS は自身の位置を示す情報を 200OK メッセージに含めて DMP に応答する．DMP はこの応答によりホームネットワーク内に存在する DMS を検出できる．

(2)　DMS を検出した DMP は，応答で得た DMS の位置情報を宛先として HTTP の GET 要求として Device Description Document メッセージを DMS へ送信する．これは DMP から DMS へのデバイス情報の取得要求となる．その応答として DMS は詳細なデバイス情報やサービス情報を XML ドキュメントとして返信する．この情報は DMP の画面に表示される．

(3)　ユーザが DMP の画面に表示されている複数の DMS から選択すると，CDS(Content Directory Service)によるコンテンツリストの要求が送信され，

コンテンツリストが DMS から応答される．

(4) ユーザがさらに HTTP GET 要求としてコンテンツを選択し，以降は DMP，DMS 間でデータ転送が行われる．

DLNA では DMP と DMS がいずれもホームネットワーク内にある状態での利用を想定しており，宅外にある DMP からホームネットワーク内にある DMS へアクセスしようとすると以下のような課題がある．(1)の手順でホームネットワークはプライベート IP アドレス空間であるためインターネット側から，通信開始ができない．また M-SEARCH メッセージはマルチキャストであるためインターネット上で使用できない．(2)の手順ではコンテンツ一覧要求の際, DMS は異なるネットワークからの接続を無視するため DMP はコンテンツ一覧を取得できない．

2.2 関連する既存技術

上記課題を解決するための既存技術として以下のようなものがある．

W-DLNA [2]は W-DLNA ゲートウェイ内で仮想 DMP を生成することにより宅外の DMP があたかもホームネットワーク内に DMS があるように認識させる方式である．W-DLNA ゲートウェイの機能が搭載されている宅外の DMP とホームネットワーク内の W-DLNA ゲートウェイが SIP シグナリング機能を有することより NAT 越えを実現する．宅外の DMP で仮想 DMS を，ホームネットワーク内の W-DLNA ゲートウェイで仮想 DMP を生成し，それが SSDP をマルチキャストすることにより実際の DMP や DMS が仮想的に相手装置を認識する．以降のメッセージは SIP を介して伝達されるが，コンテンツの再生は SIP を介さず直接 HTTP で実行する．この方式では SIP サーバをインターネット上に新たに置く必要があり，接続環境が複雑になる課題がある．

Mobile-WD(Wormhole Device) [3]では宅外の端末に Mobile-WD というソフトウェアを搭載し, Mobile-WD とホームネットワーク内の WD を通じてホームネットワーク内の DMS へアクセスする．Mobile-WD は SIP UA(User Agent)やコンテンツ表示機能および DMP との連携機能があり，宅外の端末は仮想的にホームネットワークを保持する．はじめ SIP により Mobile-WD と WD はシグナリングを行う．このとき WD のあるホームネットワークの GW として UPnP-IGD を介して行われ，また Mobile-WD と UPnP-IGD(Internet Gateway Device)はポートマッピングを行い，NAT 越えを実現する．SSDP によるデバイス検出は WD が行う. UPnP Proxy を Mobile-WD と WD 内で起動させ，CDS など各種メッセージやパケットの転送を行う．この方式は W-DLNA と同様インターネット上に SIP サーバを，ホームネットワークに WD を置く必要があり，接続環境が複雑になる課題がある．

モバイル GW [4]ではモバイル GW の導入により宅外のモバイル端末とホームネットワーク内の DLNA 対応機器とで通信する方式. モバイル GW はホームネットワーク内におき，宅外のモバイル端末からのパケットを DLNA 対応機器へ中継する．モバイル GW はユーザを SSL により認証する．また，フィルタリングにより宅外デバイス毎に表示最適化を行う．この方式は携帯端末に DMP 機能を搭載する必要がない．しかし，ホームネットワーク内のデバイスのうち非 DLNA のデバイスは利用することができない．

ポケット U [5]では携帯電話等モバイル端末からポケット U のソフトウェアをインストールした PC に保存されているコンテンツを利用する方式である．ポケット U のソフトウェアは，インストールした宅内 PC 内に保存してあるメディア

コンテンツを各宅外 DMP に最適なメディアコンテンツに変換し，宅内 PC と携帯電話網を VPN 接続する機能を持つ．認証はユーザ名とパスワードにより行う．ネット家電プラグインをインストールすることで，ホームネットワークにある DLNA 準拠 DMS に保存されているコンテンツを利用することが可能となる．この方式を利用する際，ポケット U のソフトウェアをインストールした PC は，常に起動している必要がある．このため複数人が宅内 PC を利用する場合，セキュリティに課題がある．

PSP(Play Station Portable)と PS3(Play Station 3)を連携する方式 [6]では事前に PS3 と PSP でサインイン ID とパスワードを用いて認証登録を行い，PS3・PSP ともリモートアクセスの設定を行う．PS3 がクライアントとして，PSP が DMP として動作する．PSP からホームネットワーク内のほかの DMS も利用することができる．PS3 が DLNA クライアントとして機能するため，ホームネットワーク内の接続環境が複雑になる課題がある．

また，いずれの方式も移動通信について考慮されていないため，アドレス変化による通信断絶に対応できない問題がある．

3. 提案方式

提案方式では NAT 越え問題を解決するために NAT-f(NAT free protocol) [7]，移動通信実現のために Mobile PPC(Mobile Peer to Peer Communication) [8]を適用する．以下にそれぞれの概要を示す．

3.1 NAT-f

図 2 に NAT-f の概要を示す．

NAT-f では，DDNS (Dynamic DNS)サーバにホームネットワーク内のサーバの名前と HGW のグローバル IP アドレスの関係を登録しておく．HGW にはホームネットワーク内のサーバ名とプライベート IP アドレスの関係を登録しておく必要がある．

宅外の端末は通信開始時に DDNS サーバに対してホームネットワーク内に存在する端末の名前解決依頼を行う．通信開始端末は HGW のグローバルアドレスを取得するが，IP 層より上位ソフトウェアには Server の FQDN を元に割り当てた仮想 IP アドレスを通知する．上位ソフトウェアは仮想 IP アドレス宛にパケットを送信することになるが，このとき通信開始端末は最初のパケットをカーネルに退避し，HGW との間でマッピングネゴシエーションを行う．このマッピング処理によって HGW は通信開始端末と Server が通信するために必要な NAT マッピングを生成する．通信開始端末はネゴシエーションにより上記マッピング情報を取得し，仮想 IP アドレスとマッピングアドレスの対応関係を示した仮想 IP アドレス変換テーブル（VAT table）を IP 層に生成する．通信開始端末は VAT(Virtual Address Translator)テーブルに基づいて通信パケットの宛先を仮想 IP アドレスから HGW のマッピングアドレスに書き換えて送信する．HGW はこのパケットを受信すると，NAT マッピングに従ってアドレス変換処理を実行し通信開始端末からの通信パケットを Server へ転送する．

したがって開始端末から Server へ送信する際の宛先 IP アドレスは，開始端末の上位ソフトウェアで V1 である．VAT によるアドレス変換によりカーネル部分での宛先が G2 となり，HGW の NAT を利用すると宛先が P1 となりパケットは Server へ到達する．この方法によりグローバル IP アドレス空間にある通信開始端末からホームネットワークにある Server への通信開始が可能となる．

3.2 Mobile PPC

図 3 に Mobile PPC の概要を示す．

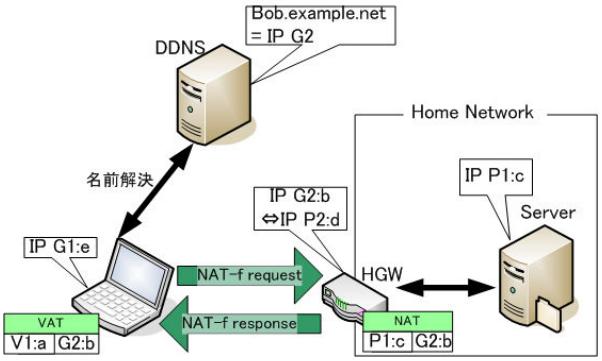

図 2 NAT-f の概要

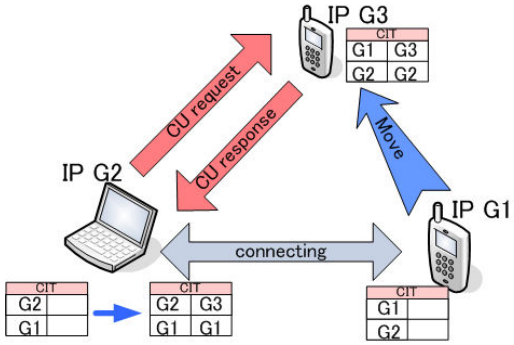

図 3 Mobile PPC の概要

IP アドレス G1 の移動端末と IP アドレス G2 の通信相手端末は IP 層に移動前後の送信元・宛先 IP アドレスの関係を示す CIT(Connection ID Table)と呼ぶアドレス変換テーブルを保持している. 図3の CIT の上段に自身の移動前後の IP アドレスを, 下段に通信相手の移動前後の IP アドレスを格納する. 移動端末が移動し IP アドレスが G1 から G3 に変化すると, 移動端末は通信相手端末の間でネゴシエーションを行い, CIT を書き換える. 以降の通信はすべてのパケットのアドレスを CIT にしたがって変換する. この方法により移動したことを移動端末・通信相手のアプリケーションが気づくことなく, 通信を継続することが可能になる.

3.3 提案方式の詳細

3.3.1 システム構成

図 4 にシステム構成を示す. グローバル IP アドレス空間に DDNS(Dynamic DNS)サーバと DMP が, プライベート IP アドレス空間であるホームネットワーク内に DMS がある. ホームネットワークとインターネットとの境に HGW がある. DDNS サーバに HGW の名前とグローバル IP アドレスを登録しているものとする. また, DMP と HGW は NAT-f と Mobile PPC に対応しているものとし, DMS は特別な機能を必要としない.

DMP が外部ネットワークにある場合, DMP と HGW 間の認証は必須である. ここでは認証にあたり, SSL を利用する. これは DMS と DMP を確実に認証するためである. したがって HGW は公開鍵証明書を取得している必要がある.

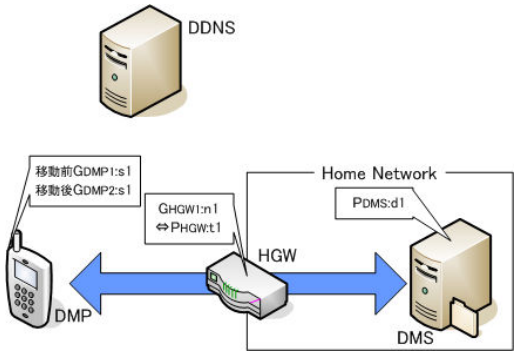

図 4 システム構成

宅外にある DMP は DDNS サーバに DMP の名前とグローバル IP アドレスを問い合わす. それらの情報を得ると DMP は SSL により HGW を認証する. DMP はSSL で得た交換鍵を用いてユーザ名及びパスワードを暗号化して送信する. HGW はパスワードを確認することにより DMP を認証する.

3.3.2 デバイス検出

認証後の提案方式のシーケンス図を**図 5** に，処理によって生成・更新したアドレス変換テーブルの内容を**表 1** に示す.

ユーザ認証後 DMP はデバイス検出を行う. 提案方式では, M-SEARCH メッセージをトリガーとしてこのメッセージを内包した NAT-f Search Request をユニキャストで HGW へ送信する(**図 5 a-1**). HGW は NAT-f Search Request を受信後, DMP の代理として M-SEARCH をホームネットワーク内にマルチキャストで送信する. このとき HGW は M-SEARCH の送信元を DMP から HGW へ書き換える処理を行う. これにより M-SEARCH メッセージの送信元が DMP から HGW となり, DMS は同一ネットワークのデバイスからのメッセージであることを認識できる. 続いて, HGW は DMS から 200OK のメッセージを受信後，そのメッセージを内包した，NAT-f Search Response を DMP へ送信する(**図 5 a-2**). DMP は受信したメッセージから 200OK を取り出し，メッセージ内の送信元 IP アドレスである DMS のプライベート IP アドレスを仮想 IP アドレス VDMS:に書き換える. 仮想 IP アドレスは HGW のドメイン名と DMS のホストアドレスを用いて重複しないように生成し， DLNA 用であることを記録しておく. ポート番号はメッセージ内に書かれていたポート番号と同じものとする.

3.3.3 マッピング処理とデバイス情報取得以降の処理

DMP のアプリケーションが仮想 IP アドレス宛にパケットを送信しようとすると，IP 層においてそのパケットを退避しておき，Mapping Request を HGW へ送信する(**図 5 b-1**). それを受け取った HGW は NAT マッピングを行う(**図 5 b-2**). 宛先 IP アドレスとして HGW のグローバル IP アドレスを DMS のプライベート IP アドレスへ，送信元アドレスとして DMP を HGW のプライベートアドレスへマッピングする NAT テーブルを生成する. その後，Mapping Response を DMP へ送信する(**図 5 b-3**).

Mapping Response を受信後, DMP は DMS の仮想 IP アドレスと Mapping Response に書かれた HGW のグローバル IP アドレスを用いて VAT テーブルを生成し NAT-f マッピングネゴシエーションを完了する(**図 5 b-4**). その後の通信は DMP において VAT によるアドレス変換，HGW において NAT によるアドレス変換を行うことにより DMP と DMS の通信が

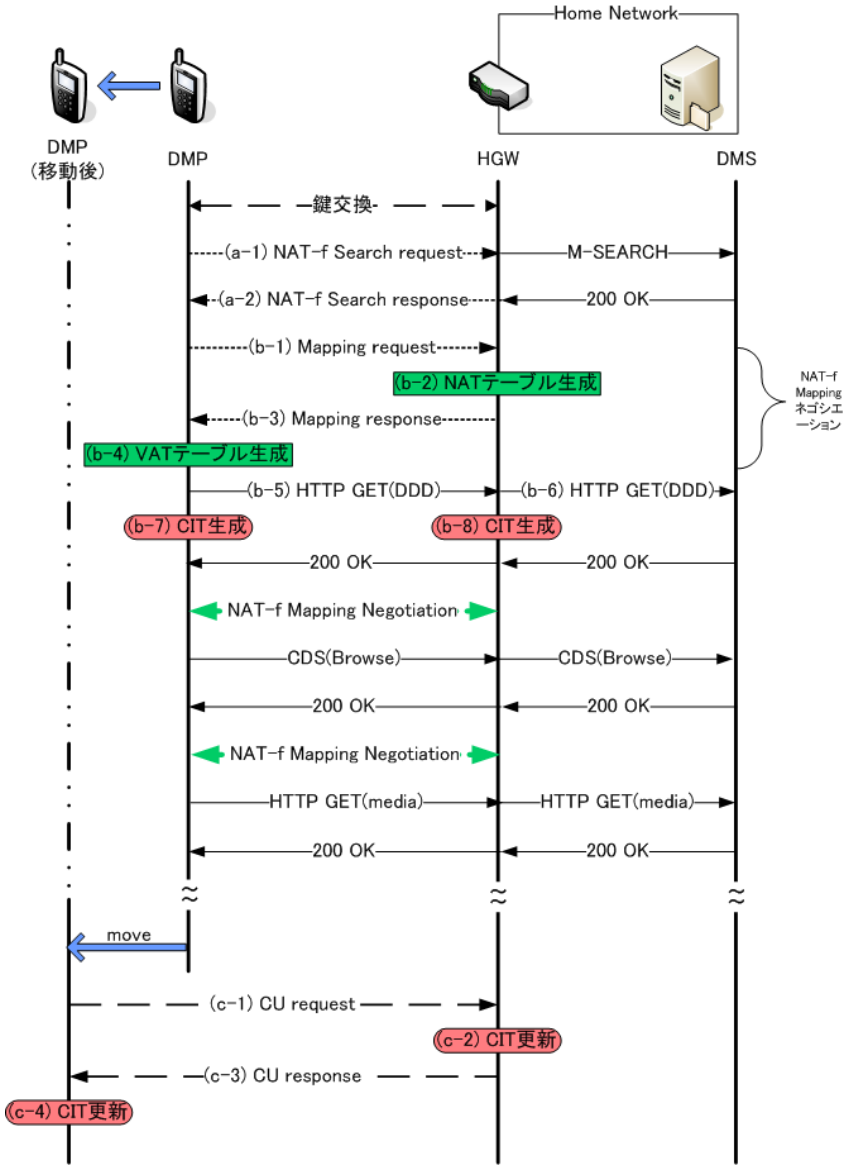

図 5 提案方式のシーケンス

行われる(**図 5 b-5,6**)．通信開始と同時に Mobile PPC で利用する CIT を生成しておく．移動先のアドレスを格納するテーブルは空である(**図 5 b-7,8**)．

以上の処理を行うことで DMP はホームネットワーク内のデバイスの情報を取得することができる．以後に続く CDS によるコンテンツ情報取得や HTTPGET によるメディア転送の動作は NAT-f マッピングネゴシエーションをその都度行ったあとに実行される．

3.3.4 移動時の処理

DMP の移動により IP アドレスが DMP から DMP2 へ変化したとき，CIT を更新する．

移動先の IP アドレスを DMP が検知すると，DMP は CU Request を HGW へ送信する(**図 5 c-1**)．これにより HGW は

DMP の移動し，その後の IP アドレスが DMP2 であることが把握できるので，その情報を元に CIT を更新する(**図 5 c-2**). 更新が完了すると HGW は DMP へ CU Response を送信する(**図 5 c-3**). これを受けて，DMP は CIT を更新する(**図 5 c-4**). 以上の処理を行う移動による IP アドレスの変化に対応することができる.

DMP のカーネル部分，HGW の IP 層でこれらの処理は行われるため，DMP のカーネル部分では，HGW のグローバル IP アドレスを CIT, VAT の順にアドレス変換しアドレス変化を隠蔽し，通信継続が可能となる．HGW では，DMP のグローバル IP アドレスを CIT, NAT の順にアドレス変換し DMS が DMP のアドレス変化を意識せずに通信を継続することが可能となる.

表 1 各テーブルの内容

(b-2)	Src	GDMP1:s1	PHGW:t1
	Dst	GHGW:n1	PDMS:d1
(b-4)	VDMS:d1	GHGW:n1	
(b-7)	DMP	GDMP1:s1	Empty
	通信相手	GHGW:n1	Empty
(b-8)	HGW	GHGW:n1	Empty
	通信相手	GDMP1:s1	Empty
(c-2)	DMP	GDMP1:s1	GDMP2:s1
	通信相手	GHGW:n1	GHGW:n1
(c-4)	HGW	GHGW:n1	GHGW:n1
	通信相手	GDMP1:s1	GDMP2:s1

4. 評価

既存技術と提案方式との比較を**表 2** に示す.

W-DLNA と Mobile WD では宅外 DMP の認証に SIP のシグナリングを利用して行っている. それに対し, モバイル GW, ポケット U, 提案方式では SSL を用いて宅外 DMP 認証している．したがって, W-DLNA と Mobile WD ではインターネット上に SIP サーバを置く必要があり, SIP サーバのセキュリティに課題がある.

提案方式とポケット U は非 DLNA 機器のコンテンツを利用することが可能であるが, W-DLNA 方式, Mobile WD 方式, モバイル GW は DLNA 機器のコンテンツしか利用することができない.

また，提案方式では今後の公衆無線 LAN の発達に対応し, 移動透過性を持つが，提案方式以外のいずれの方式も移動透過性を持たない. モバイル GW 方式やポケット U 方式，W-DLNA 方式は携帯電話網を利用しなければならない.

導入にあたり，Mobile WD 方式ではホームネットワーク内に WD が必要であり環境が複雑になる. ポケット U 方式を利用する際, ポケット U のソフトウェアをインストールした PC は，常に起動している必要があり宅内 PC が複数人で利用されている場合にポケット U 利用の制限となる可能性がある.

表 2 既存技術の比較

	W-DLNA	Mobile WD	モバイル GW	ポケット U	提案方式
認証処理セキュリティ	SIP	SIP	SSL	SSL	SSL
ホームゲートウェイの変更	必要	不要	不要	必要	必要
非 DLNA への対応	×	×	×	○	○
移動透過性	×	×	×	×	○

5. まとめ

本稿では宅外にある DLNA 準拠 DMP からホームネットワーク内にある DLNA 準拠 DMS へのアクセスを可能とし，かつ DMP の移動通信にも対応可能な方式を提案した．提案方式では，ホームネットワーク内にある DLNA 準拠デバイス以外のデバイスに保存するコンテンツを DMP が利用することができること，移動しながら通信することが可能であることを特徴とする．

今後は実装とその評価を行う予定である．

6. 参考文献

1) Digital Living Network Alliance http://www.dlna.org/home

2) 小山卓視,呉敬源,武藤大吾，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 UBI Technical Report Vol.2008 pp.1-8，No.18 (2008).

3) 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”， 電子情報通信学会 NS Technical Report Vol.107,No.6, pp.71-76 (2007).

4) 吉川貴，三宅基治，竹下敦，“モバイル連携ホームゲートウェイシステム”情報処理学会 SIG Technical Report MBL Vol.2006 No.120，pp.97-102 (2006).

5) ポケット U | サービス・機能 | NTT ドコモ http://www.nttdocomo.co.jp/service/music_movie/pocket_u/index.html

6) PS3™ | リモートプレイをする（インターネット経由） http://manuals.playstation.net/document/jp/ps3/current/remoteplay/remoteinternet.html

7) 鈴木秀和，宇佐見庄五，渡邊 晃：外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌，Vol.48，No.12，pp.3949−3961 (2007).

8) 竹内元規，鈴木秀和，渡邊 晃：エンドエンドで移動透過性を実現する Mobile PPC の提案と実装，情報処理学会論文誌，Vol.47，No.12，pp.3244−3257 (2006).