GSRA を用いた遠隔 DLNA 通信方式の提案

堀　田　直　紀

家電同士を相互接続するためのガイドラインとして DLNA(Digital Living Network Alliance) が策定されて以来, DLNA 準拠の情報家電が普及し始めている． ーザはホームネットワークにおいて, ビデオや写真, 音楽などのコンテンツの共有を行うことができるようになった．しかし DLNA は同一ホームネットワークに存在する機器同士でなければ利用することができないという課題がある．そのため, 外出先や訪問先ネットワークにおいてもコンテンツの共有を行いたいという要求がある．本稿では, それらの問題を GSRA(Group-based Secure Remote Access) の基本的な機能と DLNA 通信を組み合わせることにより, 解決する方式を提案する．提案方式では, 自宅のホームゲートウェイを変更するだけで実現することができる．

Proposal of Remote DLNA Communication System for GSRA

NAOKI HOTTA

As a guideline DLNA (Digital Living Network Alliance) since it was formulated, DLNA has started to spread information appliances compliant users in home networks, video and photos, can now be made to share content such as music or. DLNA But there is a problem of not being able to use equipment must be present between the same home network. Therefore, the scheme has been proposed that make sharing content as before and go in the visited network. In this paper, these problems GSRA (Group-based Secure Remote Access) into the basic features DLNA proposes a method for connecting with each other in spite of being outside the home network by combining communication. In the proposed scheme for DLNA devices to enable the use of all existing equipment as well as a home network so that communications can be started simply by changing the home gateway of the home.

1. はじめに

HDD レコーダやパソコン, オーディオなどのディジタル情報家電が普及し始め, それらをネットワークに接続することによって, ビデオや写真･音楽といったあらゆるデジタルコンテンツを視聴するケースが増えてきている．その中でも, 異なるメーカ間の機器の接続を容易にするためのガイドラインとして, DLNA(Digital Living Network Alliance) がある．DLNA 対応機器をホームネットワーク内において接続すると, DMP(Digital Media Player) を利用するだけで, コンテンツを保存している DMS(Digital Media Sever) を自動認識し, 利用することができる．2003 年 6 月発足以来 DLNA 準拠の製品は増え続けており, DLNA のロゴが記載されている製品同士を選べば, あらゆるデジタルコンテンツを, 共有できるようになる．

しかし, DLNA ガイドラインでは利用できる範囲は家庭内のみに限定されており, 宅外のネットワークから利用することができない．DLNA では, デバイス検出の際にマルチキャストを用いているので, インターネットを介しての通信を行なうことができない．また, TCP/IP では一般にグローバルアドレス側からプライベートアドレスに向けて通信開始ができない．これは NAT 越え問題と呼ばれ, 宅外宅外からの通信をする際の大きな課題となっている．さらに, DMS は同一ホームネットワーク以外からのアクセスを拒否する仕様となっており, 宅外の DMP と通信することができないなどの問題がある．

外部ネットワークから DLNA 端末を利用できるようにするための既存技術として各ホームゲートウェイに独自の機能を実装し, SIP セッションにより通信を可能とする方式 (W-DLNA[1]:Wide area-DigitalLiving Network Alliance,WD[2]:Wormhole Device), 無線 LAN 対応の携帯電話がコントローラとしての役割を果たし通信を可能とする方式 (MH2H[3]:Mobile Home to Home) など様々な手法が提案されている．しかし, 各ホームネットワークのゲートウェイの仕様を変更したり DLNA 準拠のデバイスしか利用することができないといった課題がある．

本稿では, これらの課題を解決するために, GSRA

(Group-based Secure Remote Access)[4] を用いて, 訪問先のホームネットワークから自宅のホームネットワークに存在する DLNA 機器に対して接続を可能とする方式を提案する．GSRA は NAT 越え技術である NAT-f(NAT-free protocol)[5] の仕組みを基礎とし, 暗号化機能やアクセス制御方式を追加することで, 安全なリモートアクセスを可能としたものである．

提案方式では訪問先ネットワークのホームゲートウェイを変更する必要がないという特長がある．

以下, 2 章で DLNA と既存技術の課題を示し, その解決方法を述べる．3 章で提案方式を述べ, 第 4 章で既存技術との比較を示し, 最後に第 5 章でまとめる．

2. DLNA と既存技術の課題

2.1 DLNA の概要と課題

DLNA とは, 家電, モバイル, パーソナルコンピュータなど異なるメーカ同士の機器の接続を容易にするために 2003 年 6 月に結成された標準化団体である．ネットワーク上に存在する機器の接続やコンテンツ共有を自動的に行い, 映像や音声データを機器間でやりとりするルールがガイドラインとして策定されている．通信プロトコルとしてデバイス検出制御の際には UPnP(Universal Plug and Play), データ転送の際には HTTP が定義されている．

図 1 に DLNA 準拠の情報家電におけるデバイス検出からコンテンツ伝送までの一連の流れを示す．

(1) デバイス検出
ユーザが DMP をたちあげると, 最初に 239.255.255.250 という DLNA 固有のマルチキャストアドレスの 1900 番ポート向けに M-SEARCH パケットを送信する．このメッセージを受け取った DMS は自分のネットワークの位置を示す OS の種類, 機器の名称などの情報を 200 OK メッセージに含めて応答する．DMP はこの応答により同一ホームネットワーク内に DMS が存在することが分かる．

(2) 機器情報の取得
応答パケットを受け取った DMP は, デバイス検出の際に取得した URL を宛先として, DDD(Device Description Document) メッセージを DMS へ送信する．要求を受け取った DMS はベンダー名, 機種名, 型番などの詳細な情報を XML ドキュメントとして 200 OK メッセージに含めて送信する．これらの詳細な情報は DMP の画面に表示される．

(3) コンテンツの探索

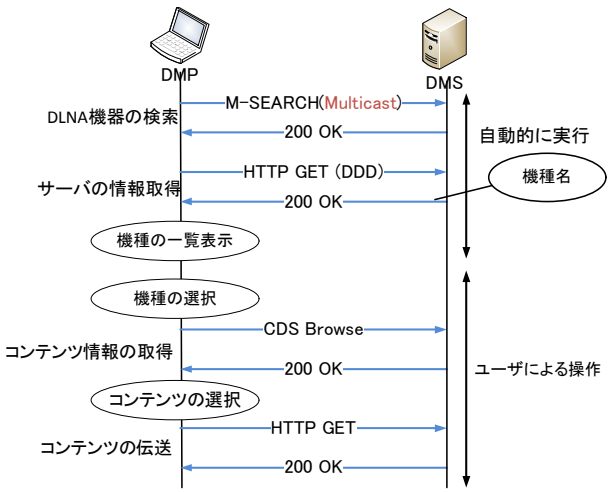

図 1 DLNA のシーケンス

これ以降は, ユーザがプレーヤの画面に表示されたアイコンや文字をクリックするといった操作に応じて, プレーヤが DMS との間でパケットをやり取りする．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) に従って Browse コマンドが送信され, DMS からコンテンツリストを取得する．

(4) コンテンツの伝送
複数あるコンテンツリストの中から, ユーザ自身が再生したいコンテンツを HTTP GET 要求として DMS に通知する．このパケットを受け取った DMS は 200 OK メッセージを送信した後, データを分割して断続的に DMP に伝送する．DMP は, 受け取ったパケットを順次再生し, コンテンツを表示する．

DLNA では DMP, 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, 宅外において利用を考えた場合には次のような技術的な課題がある．

(1) プライベートネットワーク上に置かれている機器に対して, グローバルネットワーク側から接続を開始することができない．(NAT 越え問題)

(2) デバイス検出を行う SSDP(M-SEARCH) メッセージは, マルチキャストで送信されるためインターネット上で利用することができない．

2.2 既存技術

同様の目的を持つ既存技術として, W-DLNA(Wide area-DigitalLiving Network Alliance), WD(Wormhole Device), MH2H(Mobile Home to Home) がある．

図 2 に W-DLNA の構成例を示す．W-DLNA は，ブロードバンドルータ，及びインターネットから情報家電にアクセスする例えば携帯電話のそれぞれに W-DLMA ゲートウェイ機能を持たせる．他の情報家電と接続するために SIP セッションを確立し，情報家電の代理として動作する仮想的な DMS, DMP を W-DLNA 内で生成する．また，ホームネットワーク内に DMS が複数存在する場合，どの DMS 対して IP パケットを転送すれば良いのか分からなくなる．そこで W-DLMA ゲートウェイは DMS が利用しているポート番号と DMS を一対一にマッピングする．

しかし，この方式は SIP セッションを確立するためにはインターネット上に SIP サーバを置く必要があり，接続環境が複雑になる．また，コンテンツが暗号化されないため情報漏えいや改ざんなどの危険性がある．さらに DLNA 準拠のデバイスにしか利用することができない．

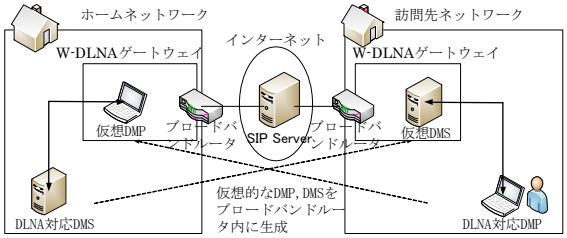

図 2　W-DLNA の構成例

図 3 に WD の構成例を示す．WD は，コネクテッドホームと呼ばれる様々な携帯機器を結ぶネットワークを実現するための構想を取り入れている．具体的には，WD と呼ぶ装置を各ホームネットワーク内に設置し，ユーザ認証，NAT ルータへのポートマッピング，DLNA 機器情報の管理，DMS/DMP 間の UPnP 通信の中継などの相互接続に必要な機能を一括して提供する．UPnP-IGD(UPnP 対応 NAT ルータ) を利用して IGD へのポートマッピングとその削除を自動的に実行することにより，NAT 越え問題を解決する．しかし W-DLNA と同様にインターネット上に SIP サーバを置く必要があるため接続環境が複雑になるという課題がある．また，DLNA 準拠のデバイスしか利用することができない．

図 4 に MH2H の構成例を示す．MH2H は，自宅の PC から携帯電話で写真や映像を視聴することができるポケット U[6] の利用シーンを拡張したサービスである．ポケット U は宅外での利用であるのに対し，MH2H は友人宅や実家といった別の家の VHN(Visited

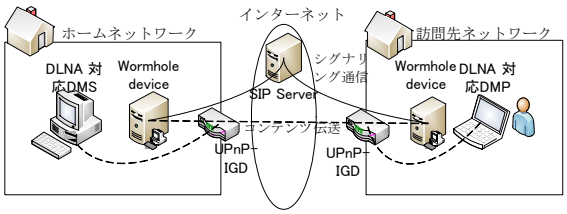

図 3　WD の構成例

Home Network) においてコンテンツを楽しむことができる．VHN 内の PD(Player Device), RD(Renderer Device) に対して，機能追加を行った移動端末と HN 内の RAG(Remote Access Gateway) とを連携させることによりインターネットを経由して PD, RD で視聴することができる．再生機器側は DLNA 準拠の製品ならよく，特別な機能追加が不要とである．しかし，コンテンツ授受を行うためには携帯電話が無線 LAN を搭載している必要がある．

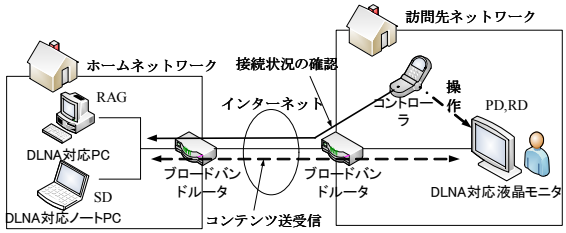

図 4　MH2H の構成例

3. 提 案 方 式

3.1 要 求 仕 様

本稿では，GSRA Router を用いることにより，訪問先ネットワークにいながら自宅ホームネットワークに存在する情報家電に対し接続を可能にする方式を提案する．2.1 で述べた課題 (1) を解決するために，GSRA Router を用いる．課題 (2) を解決するために，SSDP(M-SEARCH) メッセージをユニキャストとして新たに定義する．

3.2 GSRA の概要

GSRA は，NAT 越え技術である NAT-f の仕組みを基盤とし，さらに暗号化機能やアクセス制御機能を追加することにより安全なリモートアクセスを可能とした方式である．通信グループを構築する方法としては GSCIP(Grouping for Secure Communication for IP)[9] を採用している．この方式では通信グループとグループ鍵と呼ぶ暗号鍵を 1 対 1 に対応付ける．通信グループを定義する場合には通信に先立って通信相手

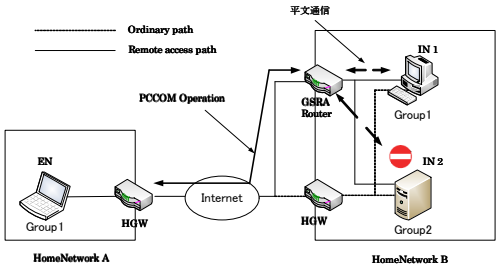

図 5 GSRA によるリモートアクセスの構成例

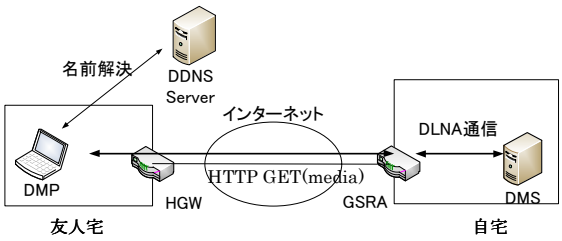

図 6 提案方式のシステム構成

とグループ情報を交換して同一グループに属している事の確認を行い, 暗号化通信に必要な動作処理情報を生成する.

図 5 に GSRA によるリモートアクセスの構成例を示す. EN(External Node) はホームルータなどの NAT 配下に存在するものとする. GSRA の機能を実装したルータを GSRA Router と呼び, 企業ネットワークのバリアセグメント上に設置する. EN は同一グループに属している IN(Internal Node)1 とは通信可能であるが, 異なるグループの IN2 との通信は許可されない. また, EN-GSRA Router 間は PCCOM(Practical Cipher COMmunication)[7] により暗号化する.

3.3 提案方式のシステム構成

GSRA はリモートアクセスを目的とした技術であるのに対し, 提案方式ではこれに DLNA 通信を加えることで, 友人先からも安全に通信が行えるようにする. 図 6 に提案方式のシステム構成を示す.

グローバル IP アドレス空間に DDNS サーバ, 異なるプライベート IP アドレス空間にそれぞれ DMP と DMS が存在している. 自宅ネットワークとインターネットとの間に GSRA の機能を備えた HGW を設置する. 訪問先の HGW には一切変更は加えない. また, DDNS Server には GSRA の名前とグローバル IP アドレス G_{GR} の関係が登録されている. 存在する DMP は外部のネットワークに存在するため, DMP と GSRA 間の認証が必須である. 提案方式では認証に SSL を用いる.

3.4 提案方式の詳細

(1) 名前解決

DMP は DMS に対する名前解決を行い, GSRA のグローバル IP アドレス G_{GR} を取得する.

(2) ユーザ認証

DMP のユーザは GSRA Router に対して認証の手続きを行う. 宅外にある DMP は, SSL によりユーザ ID とパスワードを送信する. 正規のユーザであることが認識できたならば, GSRA Router はその旨を返信し, 共通の暗号鍵 CK と各通信グループに対応したグループ鍵 GK を共有する. 暗号鍵 CK はこれ以降の処理にあるバインディング処理とマッピング処理を暗号化するものであり, グループ鍵 GK は通信グループを構築するために必要な鍵である.

(3) デバイス検出

ユーザの認証後デバイスの検出を行う. DMP はアプリケーション領域からカーネル領域に M-SEARCH をマルチキャストの要求を出す. DMP はカーネル層において M-SEARCH を受信すると, 新たに定義したメッセージ M-SEARCH Request をユニキャストでカプセル化し, GSRA Router へ送信する. ここでは, ユーザ ID, パスワードの他に, DMP が通信したい DMS のホスト名と自身のグループ情報も一緒に送信する. GSRA Router はこのメッセージを受信すると, メッセージを確認し, DMP, DMS が同一のグループに属しているかの認証を行う. 認証が成功した場合は, NAT マッピング用のポート番号 t を予約しておき, M-SERCH Response を DMP に送信する. DMP は M-SEARCH Response からポート番号 t を取得し, VAT テーブル及び PIT(Process Information Table) を仮生成する. また, DMS のプライベート IP アドレスを仮想 IP アドレス V_{DMS} に書き換える. PIT とはパケット処理内容を記載した動作処理情報テーブルのことである.

(4) バインディング処理

DMP は自身の P_{DMP}:s とあて先となる G_{GR}:t を記載したバインディング要求を GSRA Router に送信する. GSRA Router がバインディング要求を受信すると, 受信メッセージの送信元である G_{HR}:m を取得し, この取得した情報をバインディング応答に載せ DMP へ送信する. この処理の結果, DMP 側に NAT が存在する場合において, マッピング処理を実行す

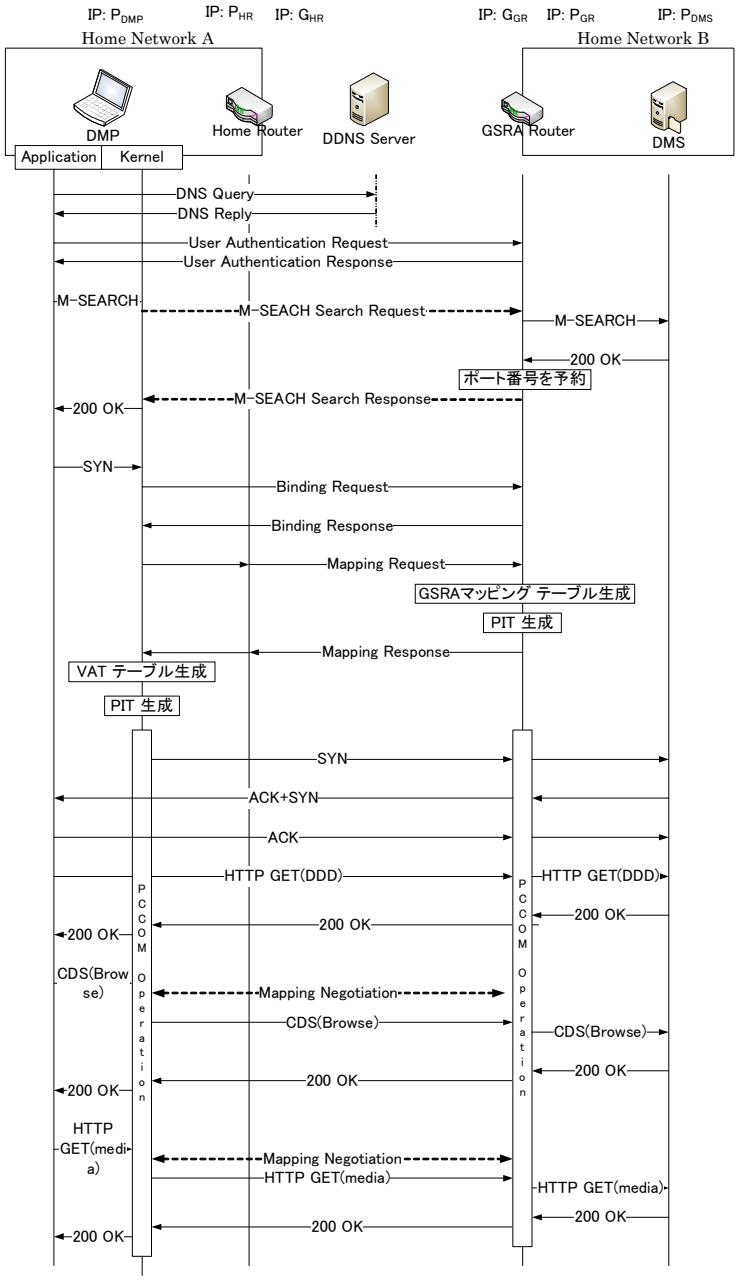

図 7 提案方式のシーケンス

ることができるようになる．

(5) マッピング処理

GSRA Router は Mapping Request から取得した情報を用いて GSRA マッピングテーブルと PIT を生成し, Mapping Response を DMP へ送信する．DMP は受信した Mapping Response から仮想アドレス変換テーブル (VAT Table) と PIT を確定する．

以後は通常の DLNA 通信と同様に, コンテンツの検索及びコンテンツ伝送の手順により, 通信が行われる．この際には PCCOM により暗号化して通信を行う．このように提案方式では GSRA Router を用いることにより, 同じグループに属した機器同士でコンテンツの共有を行うことができる．

表 1　既存技術の比較

比較項目	WD	W-DLNA	MH2H	提案方式
DMP と HGW 間の認証	SIP	SIP	SSL	SSL
コンテンツ伝送時の暗号化技術	ESP	×	×	PCCOM
非 DLNA 機器への対応	×	×	×	○
訪問先ゲートウェイの変更	必要 (×)	必要 (×)	不要 (○)	不要 (○)

4. 評　　価

表 1 に既存技術と提案方式との比較を示す．WD と W-DLNA では訪問先ネットワークに存在する DMP の認証に SIP を利用している．それに対し MH2H と提案方式では SSL を用いて認証を行っている．SSL とはインターネット上で情報を暗号化して送受信するプロトコルである．SIP はプレーンテキストで記述されているため, 内容の取得や理解が容易である．そのためセキュリティに課題がある．

WD ではコンテンツ伝送時には ESP(Encapsulating Security Payload) を, 提案方式では PCCOM により暗号化しているが, W-DLNA と MH2H は暗号化されていない為, 情報漏えいや改ざんが懸念される．

提案方式ではプライベートアドレスのネットワークに存在するすべての情報家電に対して通信が可能であるが, 他の既存技術では DLNA に準拠した製品でなければ通信を行うことができない．また, 提案方式と MH2H では訪問先のゲートウェイは一切変更は加えず, 自宅のホームゲートウェイのみ変更する．WD と W-DLNA では両ホームネットワークのホームゲートウェイを変更しなければならない為, 任意の友人宅のような環境下においては利用することが困難である．MH2H は DMP 側の機器は無線 LAN に対応した携帯電話でなければならないので, 利用できる端末が限られる．

5. ま と め

本稿では, 訪問先ネットワークの DMP から, 自宅にある DMS に対するアクセスを実現する方法を提案した．提案方式では, 訪問先のホームゲートウェイには一切変更を加える必要がない．また, DLNA 準拠のデバイス以外にもアクセスが可能である．今後は, 実装とその評価を行う予定である．

6. 参 考 文 献

[1]　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)

[2]　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, pp134-138 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, pp3949-4961(2007)

[3]　三宅基治, 吉川貴, 竹下敦：異なるホームネットワーク間でコンテンツ視聴制御技術 NTT DOCOMO テクニカル・ジャーナル Vol．16 No．3

[4]　鈴木健太, 鈴木秀和, 渡邊晃：NAT 越え技術を応用したリモートアクセス方式の提案と設計, マルチメディア, 分散, 協調とモバイル, (DICOMO2010) シンポジウム論文集, Vol．2010, No．1, pp．288-294, July．2010

[5]　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, pp3949-3961(2007)

[6]　ポケット U—サービス・機能—NTT ドコモ, http://www.nttdocomo.co.jp/service/musicmovie/pocketu/index.html

[7]　増田真也, 鈴木秀和, 岡崎直宣, 渡邊晃：NAT やファイアーウォールと共存できる暗号通信方式 PCCOM の提案と実装, 情報処理学会論文誌, Vol．47, No．7, PP．2258-2266(2006)

[8]　Digital Living Network Alliance http://www2.dlna．org/

[9]　CEAREC JAPAN 2008：ケータイ DLNA で実家や友達の家も自宅のリビングに, ドコモの MH2H http://plusd．itmedia．co．jp/mobile/articles/0810/02/news108．html

[10]　鈴木秀和, 渡邊晃：NAT-f を用いたホームネットワーク相互間接続方式の検討 ” マルチメディア, 分散, 協調とモバイル (DICOMO2008) シンポジウム論文集, Vol．2008, No．1, pp．1675-1682, July．2008