NAT-fを用いたホームネットワーク間相互接続方式の検討

鈴木秀和[†1] 渡邊晃[†1]

DLNA（Digital Living Network Alliance）準拠の情報家電機器が普及し，ユーザはホームネットワーク内の機器間で容易にメディアコンテンツを共有することができるようになった．しかしDLNAは規格上，同一ネットワーク内でしか利用することができない．そのため，インターネットを経由して他のホームネットワークやモバイル機器からホームネットワーク内のDLNA機器とコンテンツを共有することを可能とした様々な方式が提案されている．本稿では筆者らが既に提案済みのNAT越え技術NAT-f（NAT-free protocol）にDLNA機能を追加するアプローチにより，ホームネットワーク内外のDLNA機器を相互に接続する方式を提案する．提案方式はDLNA機器だけでなく，ホームネットワーク内の全ての機器に対して宅外から通信を開始することができる．

A Study of an Interconnecting Method between Home Networks Using NAT-f

Hidekazu Suzuki[†1] and Akira Watanabe[†1]

Digital Living Network Alliance (DLNA) certified consumer electronics has been spreading, and user can easily share media contents between devices in the home network. However, the DLNA architecture works only on the home network due to its guideline. In order to realize sharing contents of devices in the home network from other home networks or from mobile devices via the Internet, various technologies have been proposed. This paper presents a new interconnecting method between DLNA devices in different home networks through an approach for adding DLNA functions to NAT-free protocol (NAT-f) that can realize NAT traversal communications. With our proposed method, user can start communication with not only DLNA devices, but all devices in the home network from the outside.

1. はじめに

デジタルTVやHDD/DVDレコーダなどのデジタル情報家電が広く普及しつつあり，ネットワーク接続機能を有する機器が多く製品化されている．このような機器は，他の情報家電やPCなどの宅内機器と相互接続が可能で，ネットワークを介したコンテンツのやりとりを行うことができる．なかでも，AV機器によるホームネットワークを実現するための標準規格として，DLNA（Digital Living Network Alliance）[1]が注目されている．ユーザは特別な設定を行うことなく，DLNA対応のプレーヤDMP（Digital Media Player）を利用するだけで，コンテンツを保存しているサーバDMS（Digital Media Server）を動的に発見し，コンテンツを容易に検索，再生することができる．

このような利便性の高い情報家電をより活用するために，宅外からでも自宅ホームネットワーク内のコンテンツにアクセスしたいという要求が高まっている．しかし，DLNAガイドラインはホームネットワークでの利用を想定して策定されているため，宅外ネットワークから利用することができない．これは以下のような理由による．すなわち，DLNAではデバイス探索および制御のために，UPnP（Universal Plug and Play）[2]を採用しており，デバイス探索のためにマルチキャストを利用するSSDP（Simple Service Discovery Protocol）[3]を用いる．しかし，SSDPのマルチキャストアドレスはプライベートスコープであるため，ホームゲートウェイ（以後HGW）を越えて転送されることはない．仮に上記課題を解決して，宅外からホームネットワーク内のデバイスを発見できたとしても，HGWがNAT機能を有し，外部からアクセスを開始することができない．これはNAT越えと呼ばれる問題で，今後のホームネットワークの普及に大きな障害となる課題である．また，ユーザからの要求に対して，DMSは自身のデバイス情報や，コンテンツリストをDMPへ通知するが，このメッセージ内に

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University

DMS のプライベート IP アドレスが記載されている．このプライベート IP アドレスはホームネットワーク内でのみ有効な値であるため，宅外の DMP はコンテンツ要求を DMS へ送信することができない．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ため，宅外の DMP と通信することができないなどの課題がある．

このような課題を解決するための既存技術として，SIP を用いてホームネットワーク間で UPnP メッセージを中継する方式[4),5)]，UPnP メッセージを独自の手法により中継する方式[6)–8)]，ホームネットワーク間に VPN を構築する方式[9)–11)] など，様々な手法が提案されている[12),13)]．これらの技術は一長一短があり，モバイル機器をサポートし，ホームネットワーク内の DLNA 機器に限らず全ての機器と安全かつ高スループットな通信を実現できる包括的な方式はない．

筆者らは NAT 越え技術として，外部動的マッピング方式を提案している[14)]．この方式では，宅外の端末がホームネットワーク内の通信機器へ通信を開始する際，宅外端末と HGW が NAT-f（NAT-free protocol）と呼ぶネゴシエーションを実行し，NAT マッピング情報を HGW に動的に生成する．宅外の端末はホームネットワーク宛の通信パケットを NAT マッピング情報に一致するように変換する．以上の処理により，低遅延かつ高スループットで自宅ホームネットワーク内の機器に対して通信を開始することを可能としている．

本稿では NAT-f をベースとして異なるホームネットワーク間に存在する DLNA 機器の相互接続方式について提案する．実現のアプローチとして，両ホームネットワークの HGW に NAT-f 機能を実装し，かつ UPnP 関連パケットを処理するための DLNA 機能を追加する．NAT-f の実装により，ホームネットワーク内のすべての機器に対して宅外から通信を開始できるようになる．ここに DLNA 機能を追加することにより，DLNA を含む広い応用範囲への適用が可能になる．

2 章で DLNA の概要と宅外から利用する場合における技術課題を示し，既存技術による解決法を述べる．また，提案方式の基礎となる NAT-f の概要についても述べる．3 章で提案方式の詳細な仕組みに加えて，モバイル機器への応用について述べる．4 章で既存技術との比較を行い，最後に 5 章でまとめる．

2. DLNA の宅外利用における技術課題

2.1 DLNA

DLNA とは情報家電同士の相互接続に関するガイドラインを策定している標準化団体である．このガイドラインに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ている．

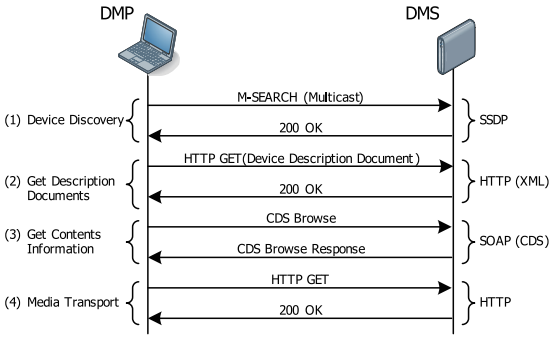


図 1 DLNA 準拠の情報家電の通信シーケンス
Fig. 1 Sequence of DLNA certified consumer electronics.

図 1 に DLNA 準拠の情報家電におけるデバイスの検出からコンテンツ再生までの一連の手順を示す．状態通知に関する手順は別途 GENA（General Event Notification Architecture）[15)] で定義されているが，ここでは省略する．

(1) **デバイスの検出**
ユーザが DMP を起動すると，DMP は SSDP で定義された M-SEARCH メッセージをマルチキャストする．上記メッセージを受信した DMS は，自身の位置を示す URL（IP アドレスとポート番号）などの情報を 200 OK メッセージに含めて応答する．DMP は応答メッセージを受信することにより，ホームネットワーク内に存在する DMS を発見できる．

(2) **機器情報の取得**
DMS を発見後，DMP は取得した URL を宛先として HTTP GET メッセージを送信し，DMS から詳細な機器情報やサービス情報を XML ドキュメントとして取得する．以上の手順により，DMP の画面に DMS の情報が表示される．

(3) **コンテンツの一覧情報の取得**
ユーザは表示された DMS を選択し，その DMS が保持するコンテンツを検索する．SOAP（Simple Object Access Protocol）[16)] 及び 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) **選択したコンテンツの伝送**
上記操作を繰り返し，ユーザは再生したいコンテンツを選択する．DMP と DMS 間は HTTP によりデータ転送が行われる．

2.2 宅外からの利用における技術課題

DLNA ガイドラインは同一ホームネットワークにおける利用を前提としており，下記に示す技術課題がある．そのため宅外からホームネットワーク上の DMS のコンテンツを利用することができない．

課題 1: 手順 (1) の SSDP ではサイトローカルスコープマルチキャストアドレスを利用しているため，DMP と異なるネットワークに存在する DMS を検出することができない．

課題 2: 手順 (1) の DMS からの応答メッセージ内には DMS のプライベート IP アドレスが記載されている．従って，DMP は DMS に対して通信を開始できない．

課題 3: 手順 (2) で DMP は DMS に対して HTTP GET によりコンテンツを要求するが，DLNA 準拠の DMS は異なるネットワークからのアクセスを無視する規格となっている．従って，DMP はコンテンツを取得することができない．

課題 1 を解決するためには，新たな手法を導入して従来の SSDP による検出の仕組みを補完する必要がある．課題 2 はグローバルネットワーク上の端末からプライベートネットワーク内の端末に通信を開始することができるように，NAT 越え問題を解決する必要がある．課題 3 を解決するためには NAT 越え通信を実現し，かつ DMS に通信相手が同一ネットワーク上に存在しているように認識させる必要がある．

2.3 既 存 技 術

本稿では異なるホームネットワーク間でコンテンツの共有を可能とする技術に着目する．なお，本節では既存技術の概要について述べ，それらの課題や提案方式との比較は 4 章で述べる．

W-DLNA[5] は W-DLNA ゲートウェイ内に仮想的な DMP 及び DMS プロセスを生成し，相互に連携することにより異なるホームネットワークやインターネット上のモバイル機器から宅内の情報家電にアクセスすることを実現している．W-DLNA ゲートウェイ同士の SIP シグナリングにより生成された仮想 DMP 及び仮想 DMS をそれぞれ DMS 及び DMP に認識させる．コンテンツリストは SIP メッセージに内包することにより中継し，W-DLNA ゲートウェイ間で転送されるメッセージの送信元を仮想 DMP または仮想 DMS に変更する．これにより，DMP 及び DMS は通信相手が同一ネットワーク内に存在する場合と同様の手順でコンテンツを再生できる．

文献 6) はワームホールデバイス（以後 WD）と呼ばれる装置をホームネットワーク内に設置し，異なる WD 同士が連携することにより，DMP は既存の通信手順のまま遠隔地にある DMS との通信を可能としている．接続先 WD に対しては SIP により機器情報の要求を行う．接続先 WD は自身のホームネットワーク内の DLNA 機器を検出し，その要約を応答する．WD は UPnP メッセージに含まれる IP アドレスを書き換えることにより，自身を DMP 及び DMS の通信相手となるように認識させる．これにより，DMP と DMS 間の通信は WD が中継することによりコンテンツの再生を可能としている．この方式は携帯端末への応用も可能である．文献 7) では WD の機能を携帯端末に実装することにより，モバイル機器からホームネットワーク内のコンテンツの再生を実現している．

Dial-to-Connect VPN システム[10),11)] や DLNA Proxy システム[9)] は HGW 間に IPsec ESP によりセキュアな VPN 通信路を形成し，その上で DMP と DMS 間の通信を行う．

文献 13) はモバイル GW と呼ぶ装置を導入し，DLNA 機器からの XML データを HTTP データに変換することにより，宅外の端末は WWW サービスと同じ要領でコンテンツを再生できるようにしている．この方式は端末が DMP 機能を保持する必要はなく，WWW ブラウザを実装していればよいため，携帯電話などのモバイル機器での利用を想定している．

これらの他に，W-DLNA と同じく SIP により UPnP メッセージを転送する拡張 DLNA メディア共有システムアーキテクチャ[4)]，UPnP メッセージを SOAP でカプセル化して転送する方式[8)]，Peer-to-Peer でコンテンツの共有を可能とする拡張 UPnP アーキテクチャxUPnP[12)] などがあり，その実現方法は多岐にわたっている．

2.4 NAT-f

筆者らが既に提案済みの NAT 越え技術として NAT-f がある．提案方式の実現に当たり重要な技術であるため，本節にて説明する．NAT-f は，通信開始端末と HGW が連携することによりホームネットワーク内の機器に対して通信を開始できる技術である．ホームネットワークに存在する既存の機器をそのまま利用でき，かつ高スループットを実現できるという利点がある．

図 2 に NAT-f の概要を示す．宅外の通信開始端末（Initiator）は通信開始時にホームネットワーク内に

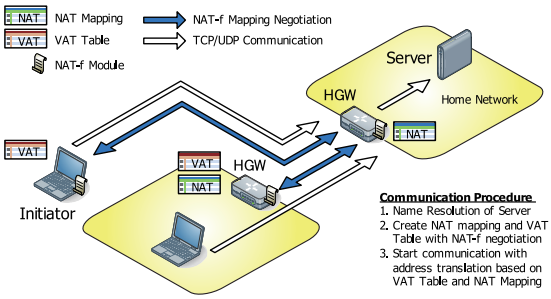


図 2 NAT-f による通信開始手順
Fig. 2 Communication procedure based on NAT-f.

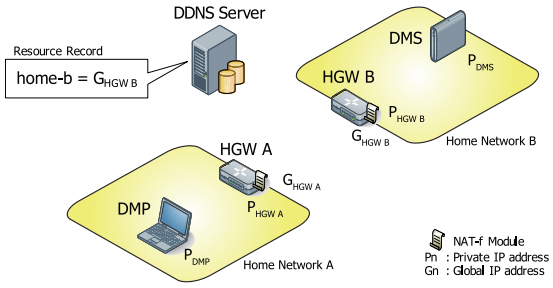


図 3 システム構成
Fig. 3 System configuration.

存在する端末（Server）の名前解決処理を行う．この過程において，Initiator は HGW のグローバル IP アドレスを取得するが，IP 層より上位ソフトウェアに対しては Server の FQDN をもとに割り当てた仮想 IP アドレスを通知する．上位ソフトウェアは仮想 IP アドレス宛に通信パケットを送信することになるが，このとき Initiator は HGW に対して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り，HGW は Initiator と Server が通信するために必要な NAT マッピングを生成する．Initiator は仮想 IP アドレスと HGW で割り当てられたマッピングアドレスの対応関係を示した仮想アドレス変換テーブル（VAT Table）を IP 層内に生成する．Initiator は VAT 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 には既に NAT マッピングが生成されているため，通常の NAT によるアドレス変換処理を実行し，Initiator からの通信パケットを Server へ転送する．

このような処理手順により，宅外の端末からホームネットワーク内の機器への通信開始を実現している．Initiator が実装する NAT-f の機能を別のホームネットワークの HGW に実装することにより，異なるホームネットワーク間の通信に応用することができる．この場合，HGW 同士でマッピングネゴシエーション及び VAT テーブルと NAT マッピングに基づくアドレス変換処理が行われる．

3. 提 案 方 式

本稿では従来の NAT-f に機能を追加するアプローチにより，異なるホームネットワークに設置された DLNA 準拠の情報家電を相互に接続する方式を提案する．2 節に示した課題 1 を解決するために，NAT-f に新たに検索要求メッセージを定義する．DMS からの応答メッセージ内に記載されているプライベート IP アドレスを仮想 IP アドレスへ書き換える．これにより，課題 2 は NAT-f を適用することにより自ずと解決される．課題 3 を解決するために，パケットの送信元アドレスを変換できるように NAT-f を拡張する．

3.1 システム構成

図 3 に本稿で想定するシステム構成を示す．提案方式を実装した異なる HGW の配下に DLNA 準拠の DMP と DMS が設置されている．本稿では装置 n のプライベート IP アドレスを “P_n”，グローバル IP アドレスを “G_n” と表記する．DDNS サーバには HGW B の名前 “*home-b*” とグローバル IP アドレス G_{HGWB} の対応関係が登録されているものとする．

このような構成において，DMP が DMS のコンテンツを共有するまでの手順を以下に示す．

3.2 ホームネットワーク間相互接続

図 4 に提案方式におけるホームネットワーク間相互接続シーケンスを示す．また，DMP と DMS 間の通信パケットの送信元及び宛先 IP アドレス，ポート番号が変化する様子を **表 1** に示す．

(1) **ユーザ認証手続き**
ホームネットワーク A（以後 Home A）のユーザは HGW B に対して認証手続きを行う．HGW A は DDNS サーバより HGW B の IP アドレスを取得してから，ユーザ ID とパスワードを送信する．HGW B はユーザ認証処理を行い，正規のユーザであればランダムなアクセスコードを生成し，返信する．HGW A は受信したアクセスコードを記録する．ユーザ認証手続きにおける通信は TLS（Transport Layer Security）[17] により保護する．

(2) **デバイスの検出**
ユーザ認証手続きを完了したら，DMP は通常の DLNA に基づく処理，すなわち M-SEARCH をマルチキャストする．HGW A は M-SEARCH を受信すると，新たに定義した検出要求メッセー

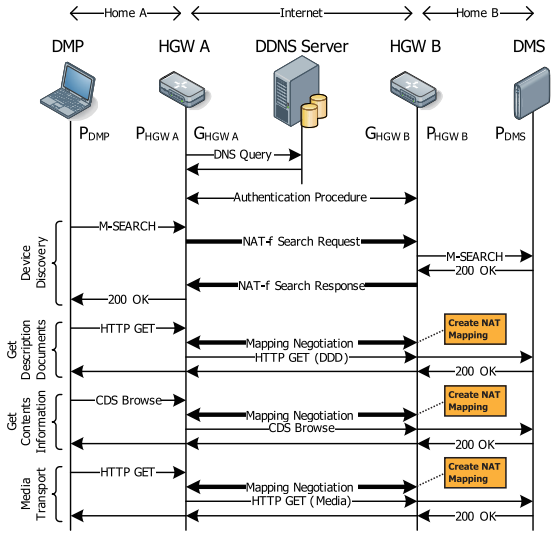


図 4 NAT-f によるホームネットワーク間相互接続シーケンス
Fig. 4 interconnecting sequence between home networks with NAT-f.

ジ Search Request を HGW B へ送信する．上記メッセージには先ほど記録したアクセスコードが記載される．

HGW B が Search Request を受信すると，記載されているアクセスコードを確認する．アクセスコードが正しければ，M-SEARCH を生成し配下ネットワーク（Home B）へマルチキャストする．ここで，M-SEARCH の送信元を HGW B とし，HGW B が DMP の代理でデバイスの検出を行う．DMS からの 200 OK を受信した HGW B は，これを内包した Search Response メッセージを生成し，HGW A へ返信する．

Search Response を受信後，HGW A は 200 OK を取り出し，メッセージ内に記載されている DMS のプライベート IP アドレス “P_{DMS}” を仮想 IP アドレス “V_{DMS}” に書き換える．V_{DMS} は Home B のドメイン名と DMS のホストアドレスを用いて生成する．なお，200 OK メッセージに IP アドレスと併記されているポート番号（ここでは “$d1$” とする）はそのままとする．その後，HGW A は割り当てた仮想 IP アドレスが DLNA 通信用であることを記録してから 200 OK を DMP に送信する．以上の処理により，DMP は他ホームネットワークに存在する DMS を検出することができる．

（3） **NAT マッピングの生成**

DMP は 200 OK により取得した仮想 IP アドレス “V_{DMS}:$d1$” を宛先とした HTTP GET メッセージを送信する．仮想 IP アドレスのネットワークアドレスは Home A と異なるため，上記パケットは必ずデフォルトゲートウェイである HGW A へ送信される．

HGW A は宛先が仮想 IP アドレスであるパケットを受信すると，NAT によるアドレス変換処理後，そのパケットを待避してから NAT-f のマッピングネゴシエーションを HGW B に対して実行する．ここで，仮想 IP アドレスが DLNA 通信用であった場合，Mapping Request メッセージに DLNA 通信用のネゴシエーションであることを示すフラグを設定する．上記フラグが設定された Mapping Request を受信した HGW B は通常とは異なる NAT マッピングを生成する．まず，宛先の DMS“P_{DMS}:$d2$” に対して HGW B の外部 IP アドレス・ポート番号 “G_{HGWB}:$n1$” をマッピングする．これは既存の NAT-f と同様である．さらに送信元の HGW A の外部 IP アドレス・ポート番号 “G_{HGWA}:$m1$” を HGW B の内部 IP アドレス・ポート番号 “P_{HGWB}:$t1$” にマッピングする．その後，HGW B は外側マッピングアドレス “G_{HGWB}:$n1$” を HGW A に通知するため，

表 1 DMP と DMS 間における通信パケットの送信元及び宛先の変遷
Table 1 Source and destination transition of communication packets between DMP and DMS.

Message	Area	Source	Destination
M-SEARCH	Home A	P_{DMP}:$s1$	M:1900
	Home B	P_{HGWB}:$t1$	M:1900
200 OK	Home B	P_{DMS}:1900	P_{HGWB}:$t1$
(SEARCH)	Home A	V_{DMS}:1900	P_{DMP}:$s1$
HTTP GET	Home A	P_{DMP}:$s2$	V_{DMS}:$d1$
(DDD)	Internet	G_{HGWA}:$m1$	G_{HGWB}:$n1$
	Home B	P_{HGWB}:$t2$	P_{DMS}:$d1$
200 OK	Home B	P_{DMS}:$d1$	P_{HGWB}:$t2$
(DDD)	Internet	G_{HGWB}:$n1$	G_{HGWA}:$m1$
	Home A	V_{DMS}:$d1$	P_{DMP}:$s2$
CDS	Home A	P_{DMP}:$s3$	V_{DMS}:$d1$
Browse	Internet	G_{HGWA}:$m2$	G_{HGWB}:$n2$
	Home B	P_{HGWB}:$t3$	P_{DMS}:$d1$
200 OK	Home B	P_{DMS}:$d1$	P_{HGWB}:$t3$
(Browse)	Internet	G_{HGWB}:$n2$	G_{HGWA}:$m2$
	Home A	V_{DMS}:$d1$	P_{DMP}:$s3$
HTTP GET	Home A	P_{DMP}:$s4$	V_{DMS}:$d2$
(Media)	Internet	G_{HGWA}:$m3$	G_{HGWB}:$n3$
	Home B	P_{HGWB}:$t4$	P_{DMS}:$d2$
200 OK	Home B	P_{DMS}:$d2$	P_{HGWB}:$t4$
(Media)	Internet	G_{HGWB}:$n3$	G_{HGWA}:$m3$
	Home A	V_{DMS}:$d2$	P_{DMP}:$s4$

M : Multicast address (239.255.255.250)
V : Virtual IP address

Mapping Response メッセージを生成し送信する．HGW A は上記メッセージを受信したら，DMS に対して割り当てた仮想 IP アドレスを HGW B の外側マッピングアドレスに変換するための VAT テーブルを生成する．

(4) **DMS への NAT 越え通信**
マッピングネゴシエーションが完了したら，待避していた HTTP GET メッセージを VAT テーブルに基づいてアドレス変換して HGW B へ転送する．HGW B は NAT マッピングに基づいて送信元および宛先の両者をアドレス変換する．さらにメッセージ内に記載されている DMP の IP アドレス “P_{DMP}” を HGW B の内側 IP アドレス “P_{HGWB}” に書き換える．この結果，HGW A から受信した HTTP GET メッセージは送信元が HGW B となり DMS へ転送される．

以上の処理により，DMS は同一ホームネットワークから要求があったと認識するため通常の DLNA の手順に従って 200 OK メッセージを返答する．DMS からの応答メッセージは上記と逆の処理により，正しく DMP へ転送される．なお，200 OK に含まれる DMS の IP アドレスは，M-SEARCH に対する 200 OK と同様に，HGW A において仮想 IP アドレスに書き換えられる．

以後のコンテンツの検索，及びコンテンツの再生時も同様の手順により，NAT 越え通信が行われる．このように提案方式は NAT-f の機能を拡張することにより，異なるホームネットワーク間において DLNA 準拠の情報家電のコンテンツを利用することができる．

3.3 モバイル機器への応用

提案方式は NAT-f の延長の技術であるため，前節で述べたホームネットワーク間だけでなく，インターネット上のモバイル端末とホームネットワーク内の DMS との間の通信に対しても全く同じ手順を適用可能である．この場合，HGW A におけるネゴシエーション処理，メッセージ内の IP アドレス書き換え処理，及び VAT テーブルに基づく仮想アドレス変換処理をモバイル端末の IP 層で行うことになる．

モバイル端末は一般に無線インタフェースによりネットワークに接続するため，通信しながら移動することが考えられる．このとき別のネットワークに移動すると IP アドレスが変化するため，通信を継続できないという課題が発生する．このような課題を解決する技術を移動透過性と呼ぶ[18]．筆者らは NAT-f と親和性の高い移動透過性技術として Mobile PPC (Mobile Peer-to-Peer Communication)[19] を提案している．NAT-f と Mobile PPC を統合することにより，NAT 越え通信と移動透過性を同時に実現する方式を提案している[20]．同様にして，提案手法に対しても上記統合を実現することが可能である．すなわち，モバイル端末がホームネットワーク内の DMS と通信中に移動しても通信を継続することが可能である．

4. 考　　察

表 2 に既存技術と提案方式の比較を示す．W-DLNA 及び WD はデバイス検出を補完する手法として SIP を用いているため，通信開始時は SIP に基づくユーザ認証を TLS 上で行うことが可能である．SIP シグナリングを受けた W-DLNA ゲートウェイは NAT マッピングを生成する．一方，WD は HGW に対して UPnP-IGD により NAT マッピングを生成する．DLNA 機器間のメディア通信は上記マッピング情報に基づいてアドレス変換処理のみが行われるため，高スループットを維持できる．しかしインターネット上の通信は暗号化されないため，情報漏洩などの懸念がある．両技術は共にモバイル機器での利用についても可能であるが，DLNA 準拠の情報家電との通信を対象とした技術であるため，非 DLNA 機器に対して NAT 越え通信を行うことはできない．

文献 7) では WD 間で IPsec による VPN を構築することにより，メディア伝送に対して暗号化通信を行うとしている．WD はホームネットワーク内に設置されるため，HGW を跨って VPN を構築することになる．従って，IKE（Internet Key Exchange）[21] と IPsec 通信の NAT 越えを実現するためにさらに UDP によりカプセル化処理を行う必要がある[22),23]．HGW 間で IPsec により VPN を構築してスループットの性能評価を行った結果が文献 9) で示されている．これによると，非 IPsec 通信に対して HGW が IPsec ハードウェア実装の場合は約 20% ，ソフトウェア実装の場合は約 90% 低下することが示されている ⋆1．従って，UDP でカプセル化することにより，さらにスループットが低下してしまう懸念がある．

D2C VPN システムと DLNA Proxy システムは HGW 間に VPN を構築することにより，DMP を DMS と同じホームネットワークに参加させる．そのため，DMP は通常の DLNA 手順により DMS を検出することが可能であり，かつインターネット上のメ

⋆1 Ethernet フレームサイズが 1350bytes の時，非 IPsec 通信のスループットは約 95Mbps であったのに対して，ハードウェア実装の場合は約 75Mbps，ソフトウェア実装の場合は約 10Mbps.

表 2 既存技術との比較
Table 2 Comparison with existing technologies.

比較項目	W-DLNA	WD/Mobile-WD	D2C VPN	DPS	提案方式
遠隔地のデバイス検索を実現する補完技術	SIP	SIP	VPN	VPN	NAT-f
メディア伝送の NAT 越え実現手法	NAT マッピング	UPnP	VPN	VPN	NAT-f
セキュリティ（ユーザ認証時）	SIP (TLS)	SIP (TLS)	SIP (TLS)	IPsec ESP	TLS
セキュリティ（メディア伝送時）	×	× (IPsec ESP $^{\star 1}$)	IPsec ESP	IPsec ESP	PCCOM
高スループットの維持	○	○ (×$^{\star 1}$)	△	×	○
非 DLNA 機器に対する通信のサポート	×	×	○	○	○
モバイル機器のサポート	○	○	×	○	○
モバイル機器における移動透過性のサポート	×	×	×	×	○
ホームゲートウェイの変更	× 必要	○ 不要	× 必要	△$^{\star 2}$	× 必要

WD: Wormhole Device[6] D2C VPN: Dial-to-Connect VPN System[11] DPS: DLNA Proxy System[9]
$^{\star 1}$ WD 間における VPN 適用時 $^{\star 2}$ VPN 非対応の場合は変更が必要

ディア通信に対して強力な機密性と認証を確保できる．また，接続先ホームネットワーク内の非 DLNA 機器との通信も可能である．しかし， IPsec ESP のカプセル化によるヘッダオーバヘッドが発生するため，スループットが低下する．D2C VPN システムでは VPN 確立前に行うユーザ認証に SIP を用いており，SIP の SDP（Session Description Protocol）指定により接続先に対して帯域確保の要求を行う．これにより，SIP のメディアチャネル上に VPN を構築することにより QoS を保証しているが，スループットの低下は避けられない．一般に，VPN を構築するシステムでは異なるホームネットワーク間でアドレスが重複しないように管理しなければならないなどの課題がある．特に後者の課題により，不特定のホームネットワーク間で VPN 方式を適用することは困難である．

提案方式は NAT-f を基盤としたシステムであるため，非 DLNA 機器との通信やモバイル機器での利用も可能である．通信開始時のユーザ認証には TLS を利用することができる．強靭な認証を要求する場合には PKI 技術を導入して，双方向認証を実現する必要がある．既存技術はメディア転送時のセキュリティを確保するために IPsec を適用するのが一般であるが，提案方式では NAT-f と親和性の高い PCCOM（Practical Cipher Communication）[24] を適用する．PCCOM はオリジナルパケットのフォーマットを変えないまま本人性確認とパケットの完全性保証を行うことができる暗号通信方式である．NAT やファイアウォールと共存でき，かつ IPsec と比較して高スループットを実現できる特徴がある．このため，提案方式の利点を損なうことなく適用可能である．

提案方式の特筆すべき特徴として，3.3 節で述べたようにモバイル機器の移動透過性をサポートできことが挙げられる．これによりユーザはホームネットワーク内のコンテンツを再生しながら移動することが可能であり，ユビキタスネットワークで求められる柔軟な通信スタイルを実現することができる．

提案方式では HGW を変更する必要がある．それに対し WD は既存の HGW をそのまま利用可能だが，ホームネットワーク内に専用機器が必要である．従って，新規に装置を導入する点においては同等である．また HGW を変更することは特別困難な課題ではない．NAT-f における HGW は NAT アプリケーションに NAT-f 機能を実現するモジュールを追加することにより実現できる．従って，既存 HGW の NAT アプリケーションをアップデートすることが可能であれば，新たに装置を導入する必要はない．

5. おわりに

本稿では異なるホームネットワーク間に存在する DLNA 準拠の情報家電が相互に接続できる方式を提案した．提案方式は既存の NAT 越え技術である NAT-f をベースとしており，DLNA 通信に対応するための機能を追加実装するアプローチにより相互接続を実現する．そのため，DLNA 準拠の情報家電だけでなく，ホームネットワーク内の全ての機器に対して宅外から通信を開始することができる．ホームネットワーク間だけでなく，モバイル機器に対しても適用可能であり，移動透過性技術と組み合わせた応用もできることを示した．

今後は提案方式の実装と動作検証を行う．また通信開始時におけるユーザ認証手続きの詳細や，DLNA ガイドラインにおいて想定されている 3-Box モデルでの利用を検討する．さらに DMC（Digital Media Controller）を用いた場合の手順について検討を深める予定である．

謝辞 本研究の一部は，日本学術振興会科学研究費補助金（特別研究員奨励費 20・1069）の助成を受けたものである．

参 考 文 献

1) Digital Living Network Alliance: *DLNA Networked Device Interoperability Guidelines Expanded* (2006). http://www.dlna.org/.
2) UPnP Forum: *Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0* (2001). http://www.upnp.org/standardizeddcps/igd.asp.
3) Goland, Y.Y., Cai, T., Leach, P., Gu, Y. and Albright, S.: Simple Service Discovery Protocol/1.0 Operating without an Arbiter, Internet-draft, IETF (1999). draft-cai-ssdp-v1-03.txt (expired).
4) 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 Transactions on Consumer Electronics*, Vol.53, No.2, pp.542–547 (2007).
5) 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，電子情報通信学会技術研究報告. NS，Vol.107, pp.71–76 (2007).
6) 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，*DICOMO2007*, Vol.2007, pp.134–138 (2007).
7) 小山卓視，呉　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，2008-UBI-017, Vol.2008, pp.1–8 (2008).
8) 小川将弘，早川裕志，小板隆浩，佐藤健哉：グローバルネットワーク環境における UPnP 機器連携の実現，*DICOMO2007*, Vol.2007, pp.125–133 (2007).
9) Kim, T., Oh, Y.J., Lee, H.K., Paik, J. E.H. and Park, K.R.: Implementation of the DLNA Proxy System for Sharing Home Media Contents, *IEEE Transactions on Consumer Electronics*, Vol.53, No.1, pp.139–144 (2007).
10) 春山敬宏，水野伸太郎，山田孝二，水野　修：VPN を介した情報家電サービス利用方式の提案，情報処理学会研究報告，2006-UBI-012, Vol.2006, pp.1–6 (2006).
11) 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) 2008*, pp. 1224–1225 (2008).
12) Venkitaraman, N.: Wide-Area Media Sharing with UPnP/DLNA, *Proc. 5th IEEE Consumer Communications and Networking Conference (CCNC) 2008*, pp.294–298 (2008).
13) 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，情報処理学会研究報告，2006-ITS-027, Vol.2006, pp.97–102 (2006).
14) 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).
15) Cohen, J. and Aggarwal, S.: General Event Notification Architecture Base, Internet-draft, IETF (1998). draft-cohen-gena-p-base-01.txt (expired).
16) Box, D., Kakivaya, G., Layman, A., Thatte, S. and Winer, D.: SOAP: Simple Object Access Protocol, Internet-draft, IETF (1999). draft-box-http-soap-01.txt (expired).
17) Dierks, T. and Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, IETF (2006).
18) 寺岡文男：インターネットにおけるノード移動透過性プロトコル，電子情報通信学会論文誌，Vol.J87-D1, No.3, pp.308–328 (2004).
19) 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).
20) 鈴木秀和，金本綾子，渡邊　晃：NAT-f の移動透過通信への拡張，*DICOMO2007*, Vol.2007, pp. 857–865 (2007).
21) Harkins, D. and Carrel, D.: The Internet Key Exchange (IKE), RFC 2409, IETF (1998).
22) Kivinen, T., Swander, B., Huttunen, A. and Volpe, V.: Negotiation of NAT-Traversal in the IKE, RFC 3947, IETF (2005).
23) Huttunen, A., Swander, B., Volpe, V., DiBurro, L. and Stenberg, M.: UDP Encapsulation of IPsec ESP Packets, RFC 3948, IETF (2005).
24) 増田真也，鈴木秀和，岡崎直宣，渡邊　晃：NAT やファイア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).

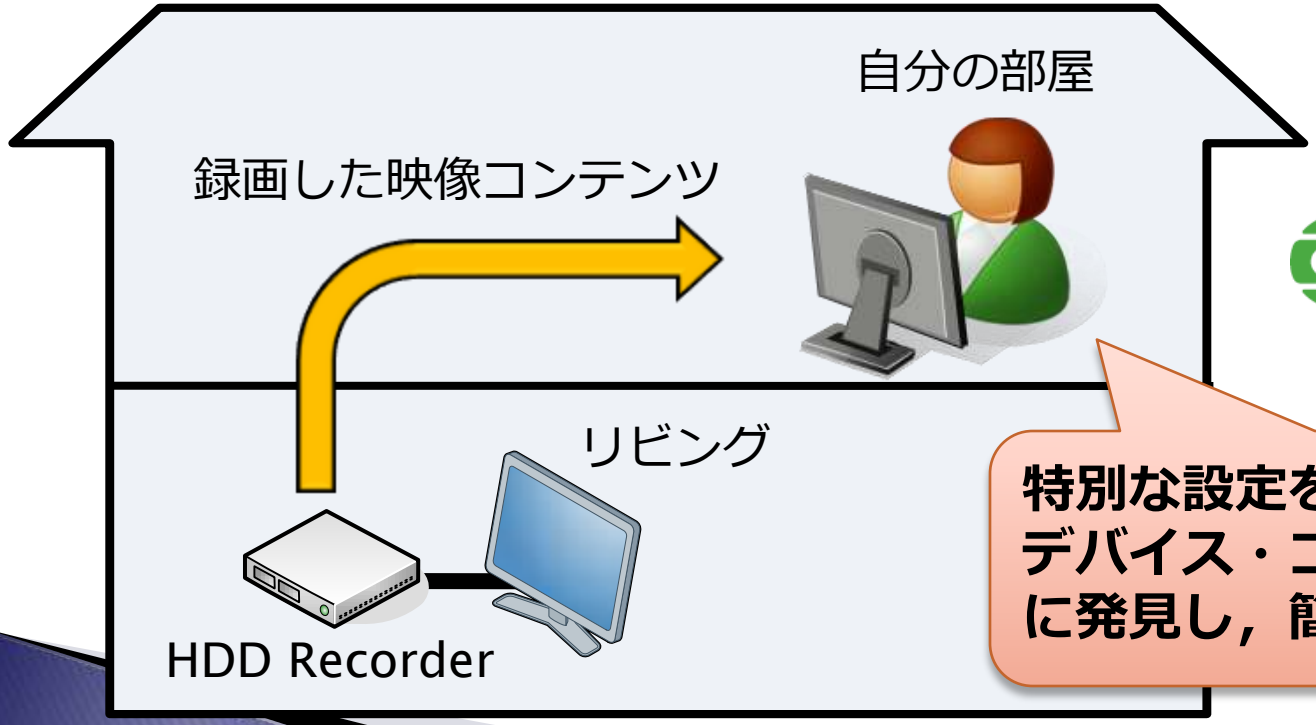
Multimedia, Distributed, Cooperative, and Mobile (DICOMO) Symposium
July 9th–11th, 2008
Program No. 7F-4

NAT-fを用いたホームネットワーク間相互接続方式の検討

名城大学大学院理工学研究科
鈴木 秀和　渡邊 晃

研究背景

- 近年，DTVやHDD/DVDレコーダなどの情報家電が広く普及
  - **DLNA（Digital Living Network Alliance）**が注目
    - UPnPやHTTPなどの標準技術を組み合わせて実現



dlna

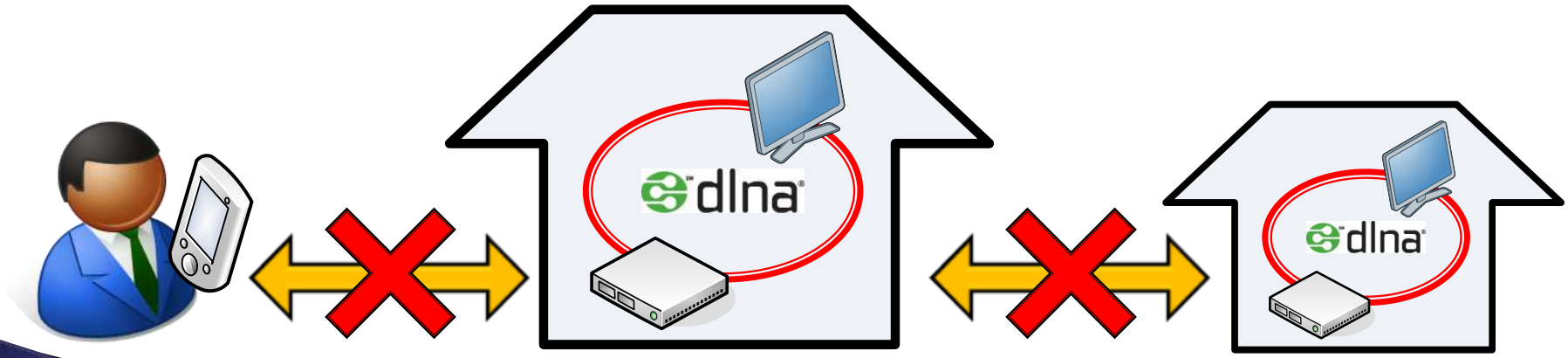
特別な設定を行うことなく，デバイス・コンテンツを動的に発見し，簡単に再生できる

研究背景

- 多様なシチュエーションでも利用したい
  - 外出先から，ホームネットワーク間で，etc.
- DLNAガイドライン

  ➔ホームネットワーク（HNW）での利用を想定した仕様

宅外からDLNA準拠機器のコンテンツを利用できない



既存技術

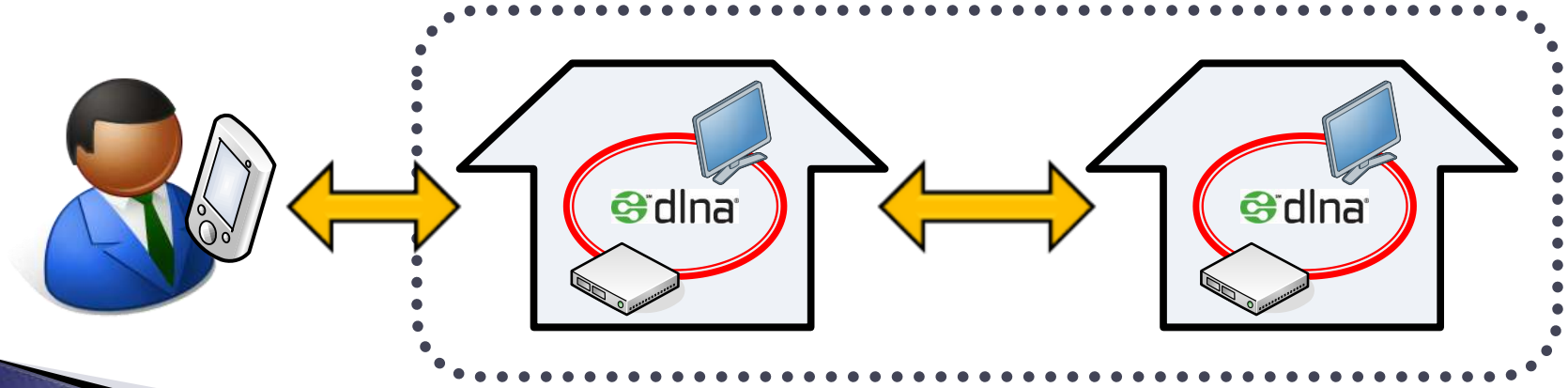
	技術・システム名	提案機関
国内	W-DLNA	KDDI研究所
	Wormhole Device	電気通信大学
	Dial-to-Connect VPN System	NTT情報流通プラットフォーム研究所
	Mobile Home Gateway System	NTTドコモ総合研究所
	UPnPメッセージのカプセル化転送	同志社大学
海外	拡張DLNAメディア共有アーキテクチャ	韓国電子情報通信研究院
	DLNA Proxy System	韓国電子情報通信研究院
	xUPnP	Motorola Labs

宅外からDLNA通信を実現するための新しい技術

本研究のアプローチ

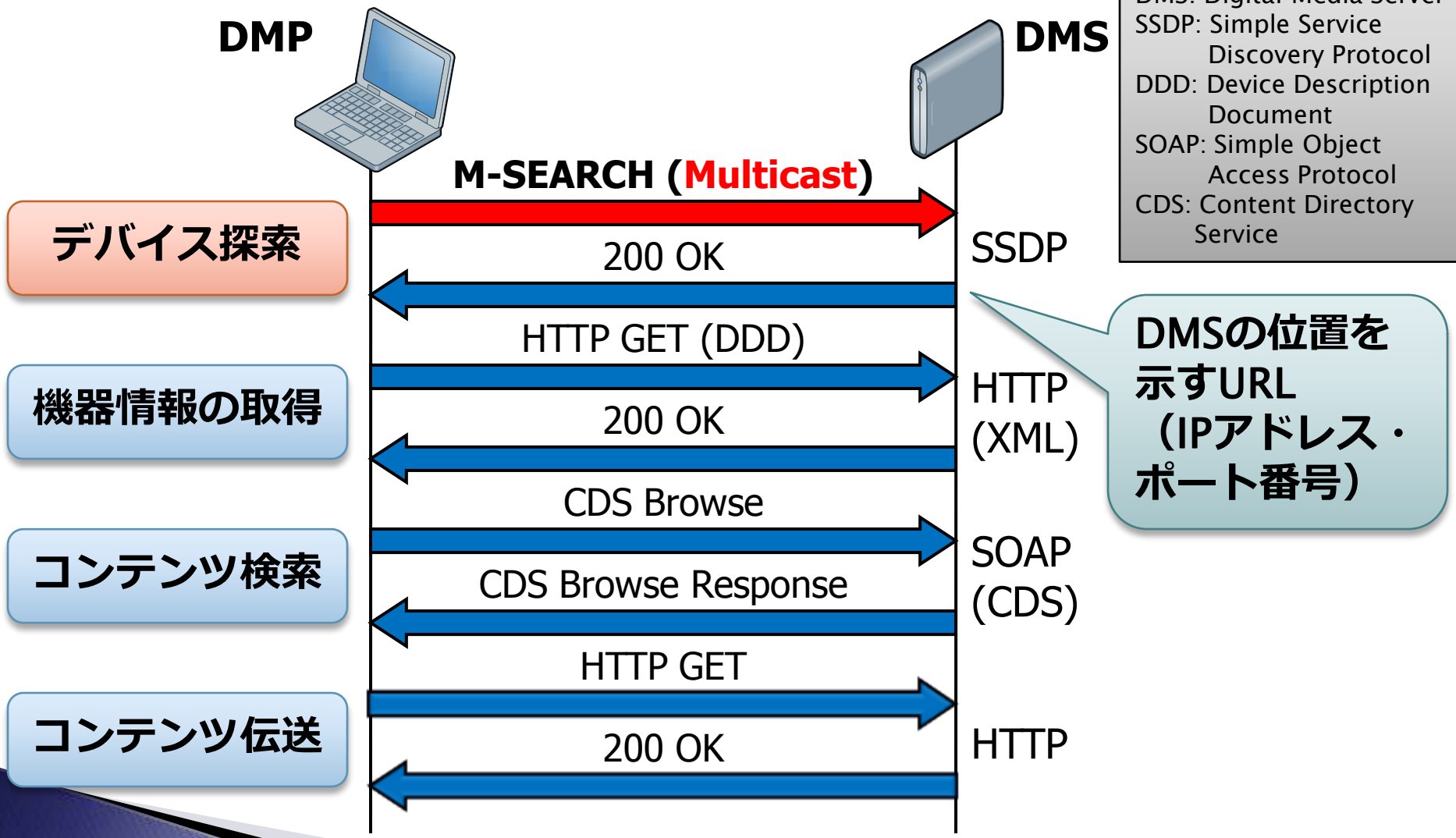
宅外からの利用＝NAT越え通信の延長と捉える

- **外部動的マッピング方式をベース**とした方法
  - NAT越え通信を実現する方式
  - 上記方式を実現する**NAT-f（NAT-free protocol）**に DLNAサポート機能を追加実装



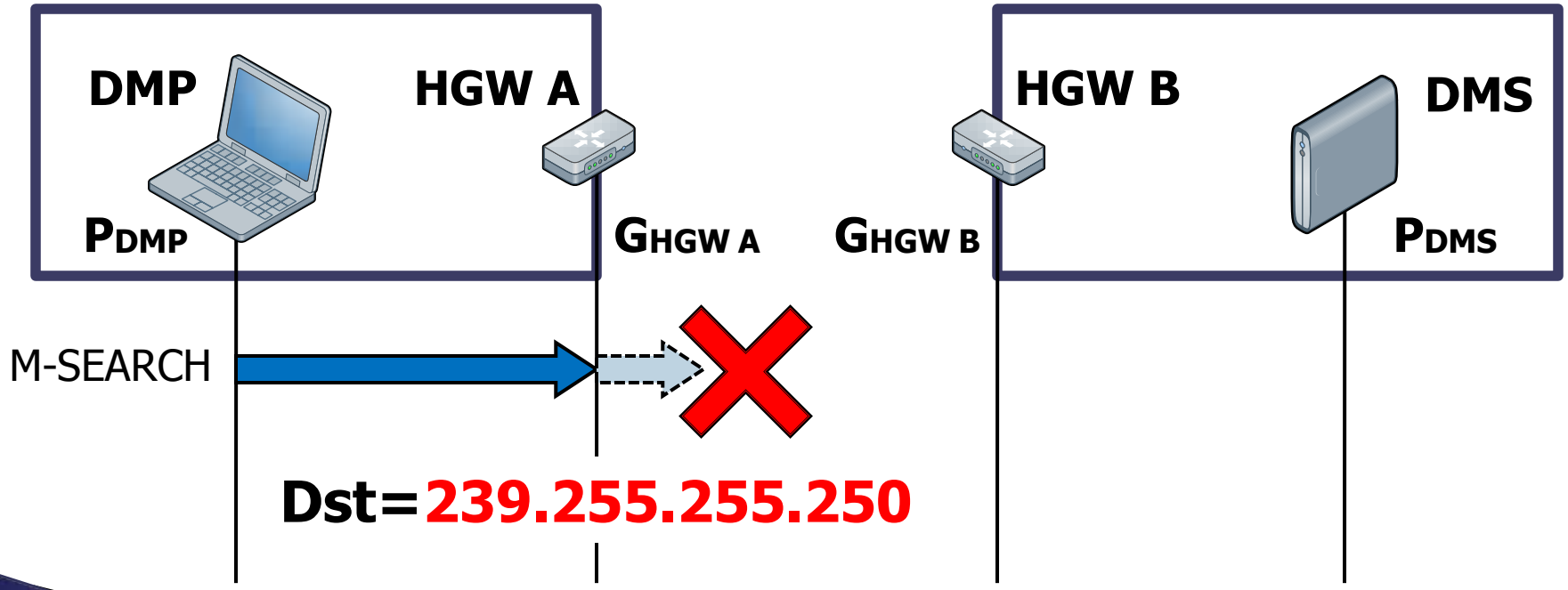
DLNAシーケンス

DMP: Digital Media Player
DMS: Digital Media Server
SSDP: Simple Service Discovery Protocol
DDD: Device Description Document
SOAP: Simple Object Access Protocol
CDS: Content Directory Service



宅外から利用できない原因１

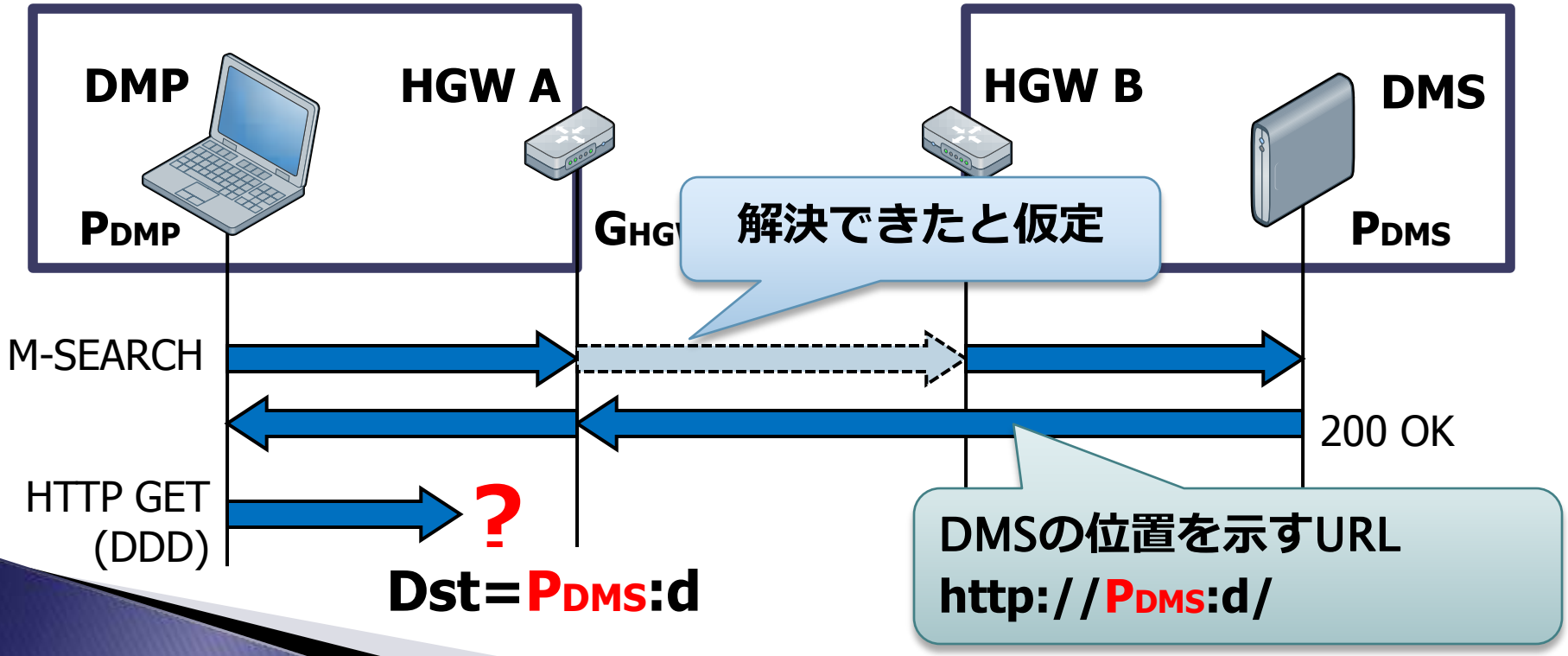
- SSDP（M-SEARCH）がローカル用マルチキャストアドレス*を利用
  - **DMPは異なるHNWにあるDMSを発見できない**



* Administratively Scoped Block (RFC2365)

宅外から利用できない原因２

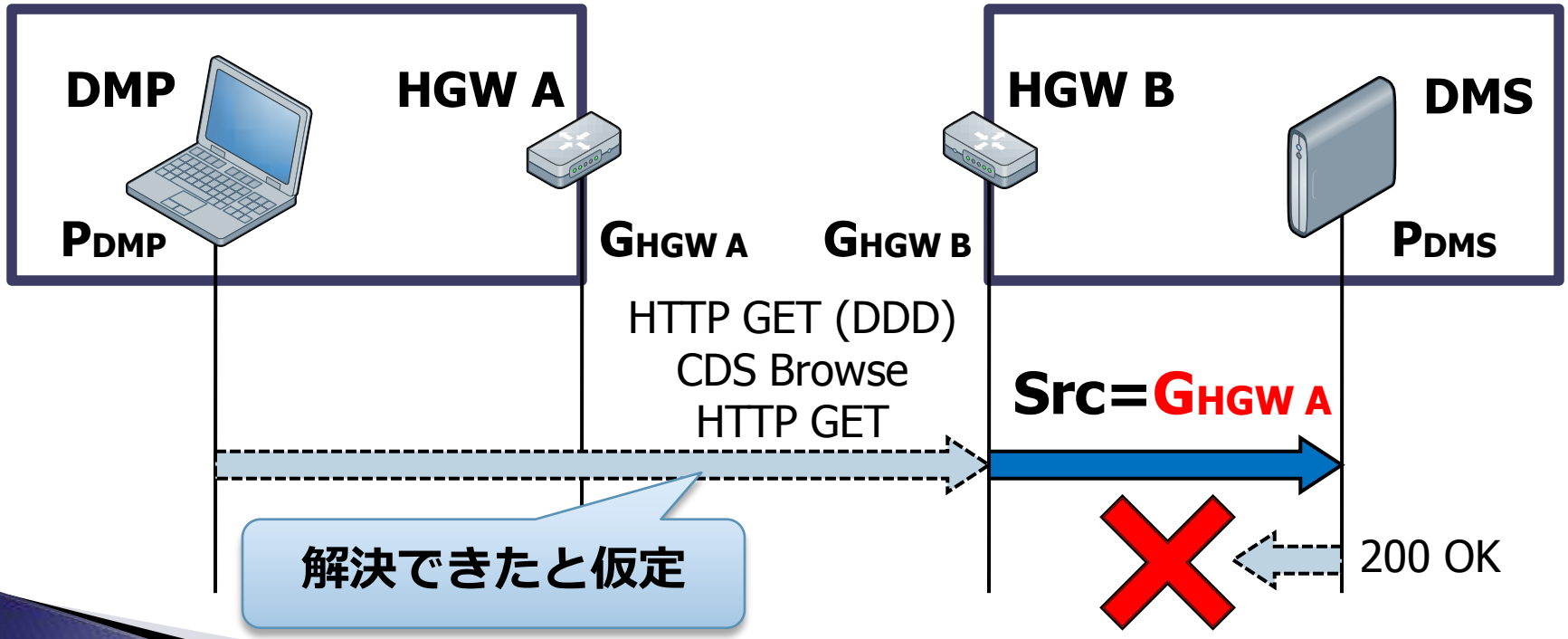
- M-SEARCHの応答としてDMSのプライベートアドレスが通知
  - **DMPはDMSに対して通信を開始できない**



宅外から利用できない原因３

- DMSは異なるNWからのアクセスを無視する規格
  - DMSから200 OKが応答されない

➔**DMPはDMSからコンテンツを取得することができない**



提案方式による課題の解決方法

- 課題１：異なるHNWのDMSを発見できない
  - NAT-fに検索要求メッセージを定義

  ➔**HGWが代理で探索**

- 課題２：DMSに対して通信を開始できない
  - DMSからの応答メッセージ内に含まれるIPアドレスを仮想IPアドレスに書き換え

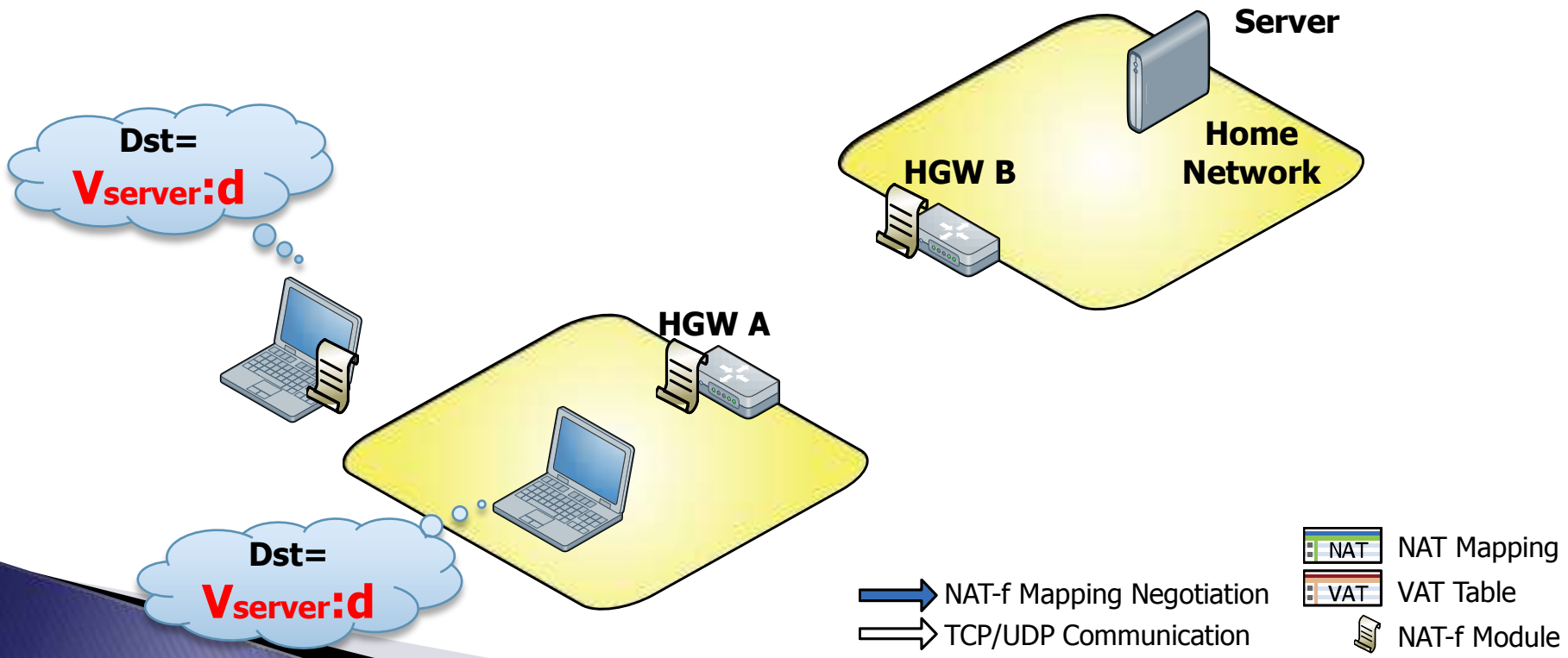
  ➔**外部動的マッピング方式によるNAT越え通信**

- 課題３：異なるNWからのアクセスを無視
  - NATのアドレス変換を拡張

  ➔**DMSに対して同一HNWからの要求として認識させる**

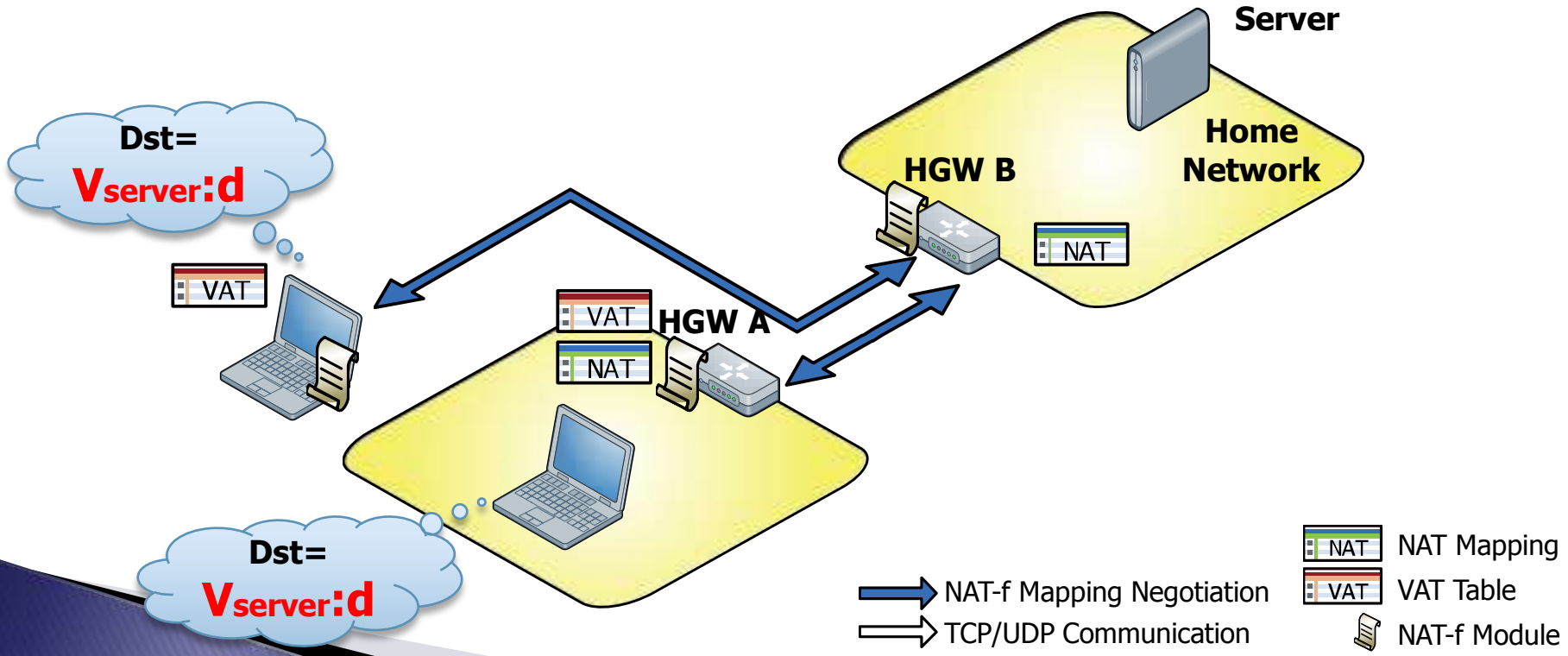
外部動的マッピング方式（NAT-f）

- HNW内の全ての機器に対してNAT越え通信を実現
  1. 通信相手を**仮想IPアドレス**として認識
     - FQDNから仮想IPアドレスを生成



外部動的マッピング方式（NAT-f）

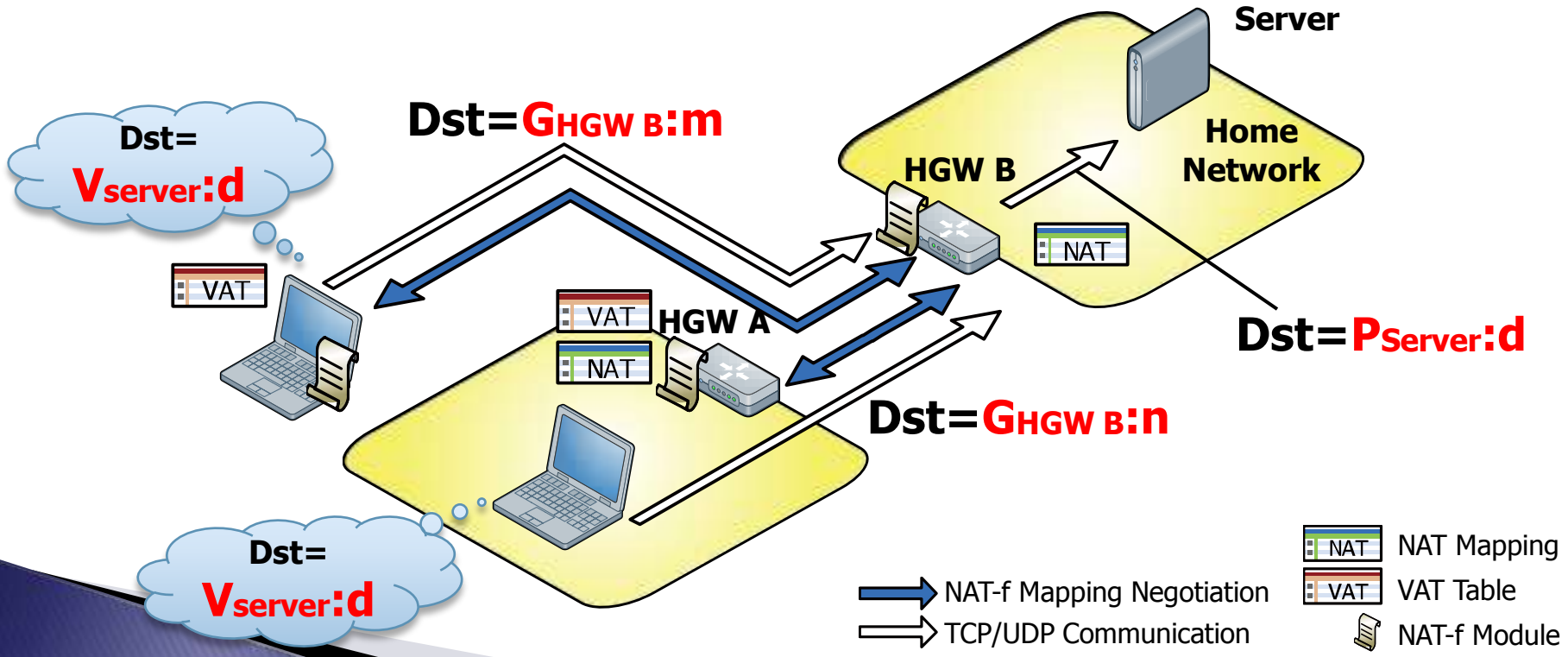
- HNW内の全ての機器に対してNAT越え通信を実現
  2. **NAT-f**によりNAT Mapping，**VATテーブル**を生成
     - NAT Mapping：Serverに転送するために必要な情報
     - VATテーブル：仮想IPアドレスを上記Mappingに変換する情報



外部動的マッピング方式（NAT-f）

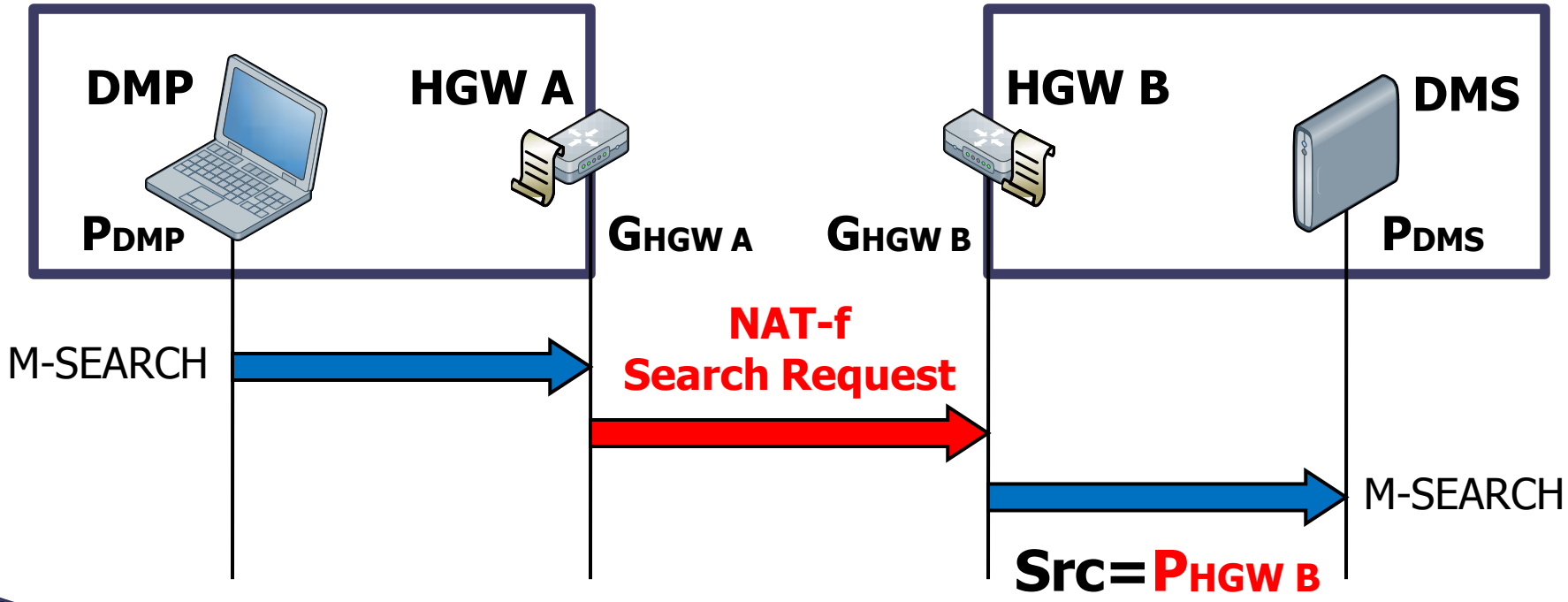
- HNW内の全ての機器に対してNAT越え通信を実現
  3. VATテーブルとNAT Mappingに基づいてアドレス変換
     - 応答は逆の変換

➔**NAT越え通信が可能**



デバイスの検出

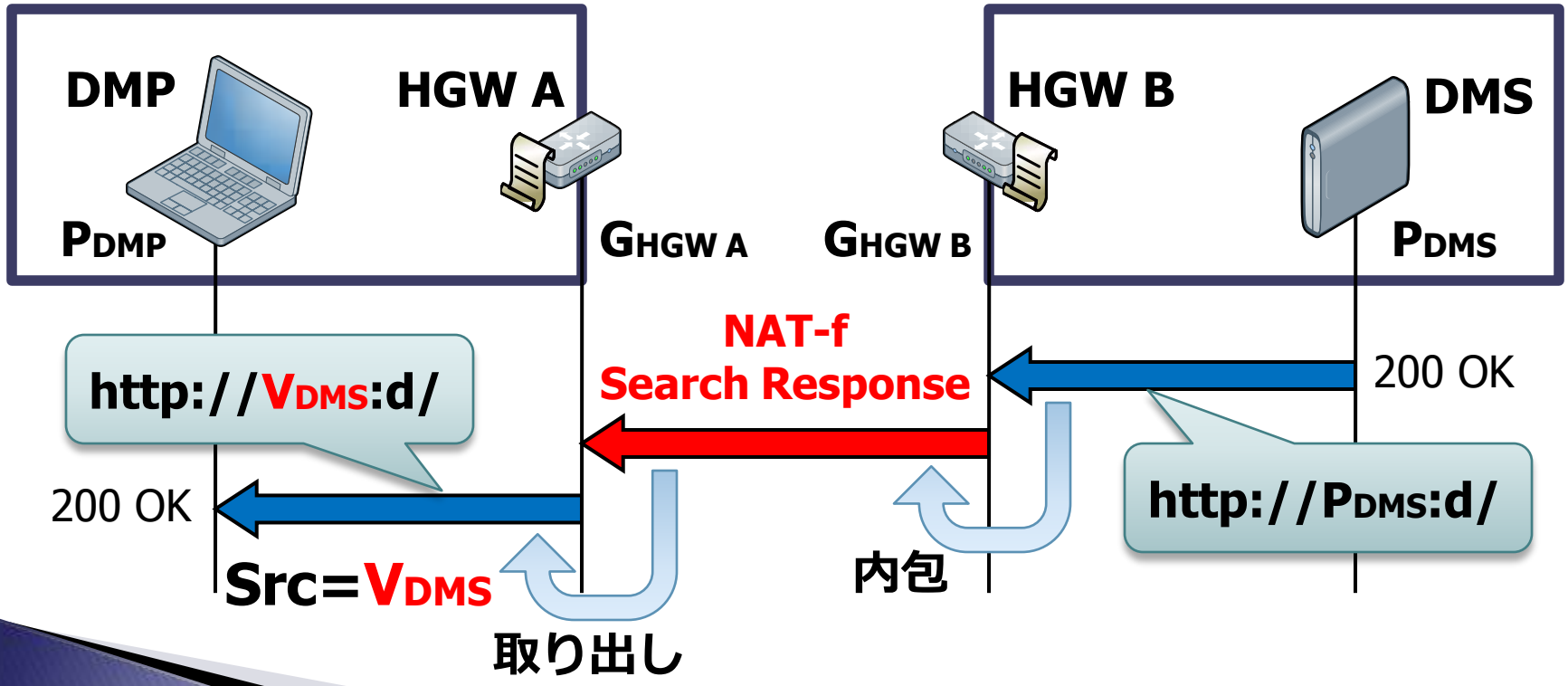
- 新たに定義した検索要求メッセージにより相手HGW Bに対して**代理でデバイス検索を要求**
  - HGW BはM-SEARCHをマルチキャスト



デバイスの検出

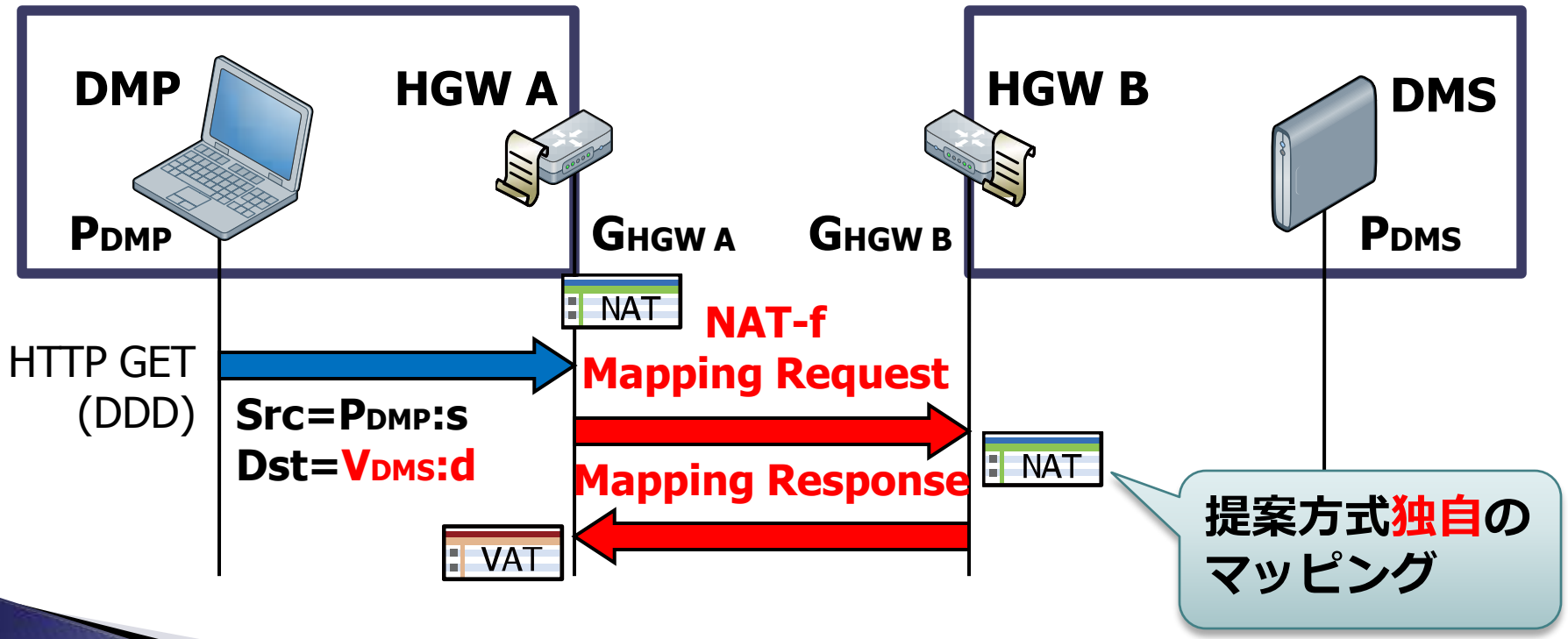
- 検出結果をHGW Aに応答（Search Response）
  - HGW AはDMSのアドレスを仮想IPアドレスに書き換え

  ➔**DMSをV_{DMS}として認識**

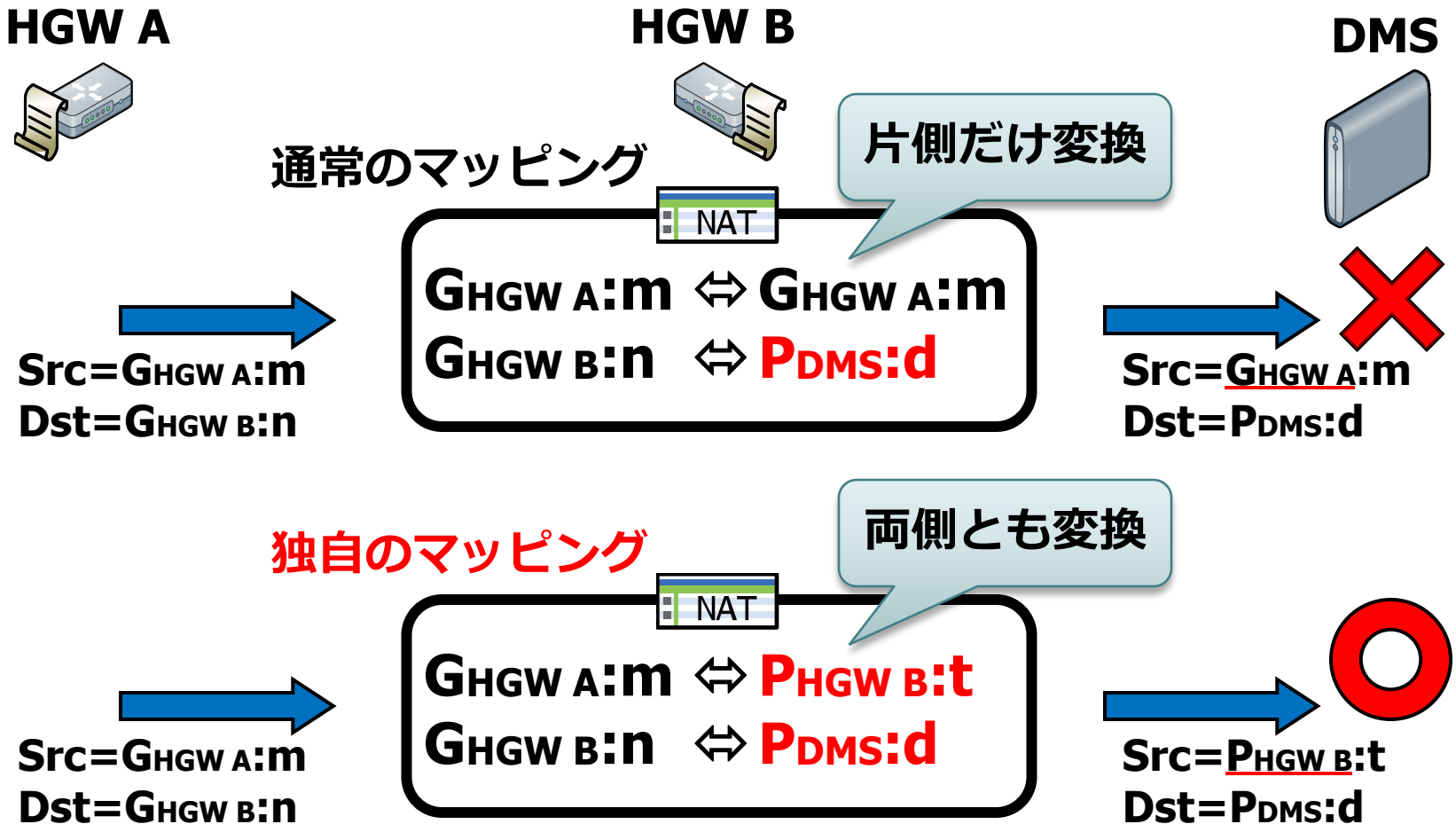


NATマッピングの生成

- NAT-f Mappingネゴシエーションを実行
  - HGW Bは**独自のNATマッピングを生成**
  - HGW Aは従来と同じNATマッピング・VATテーブルを生成



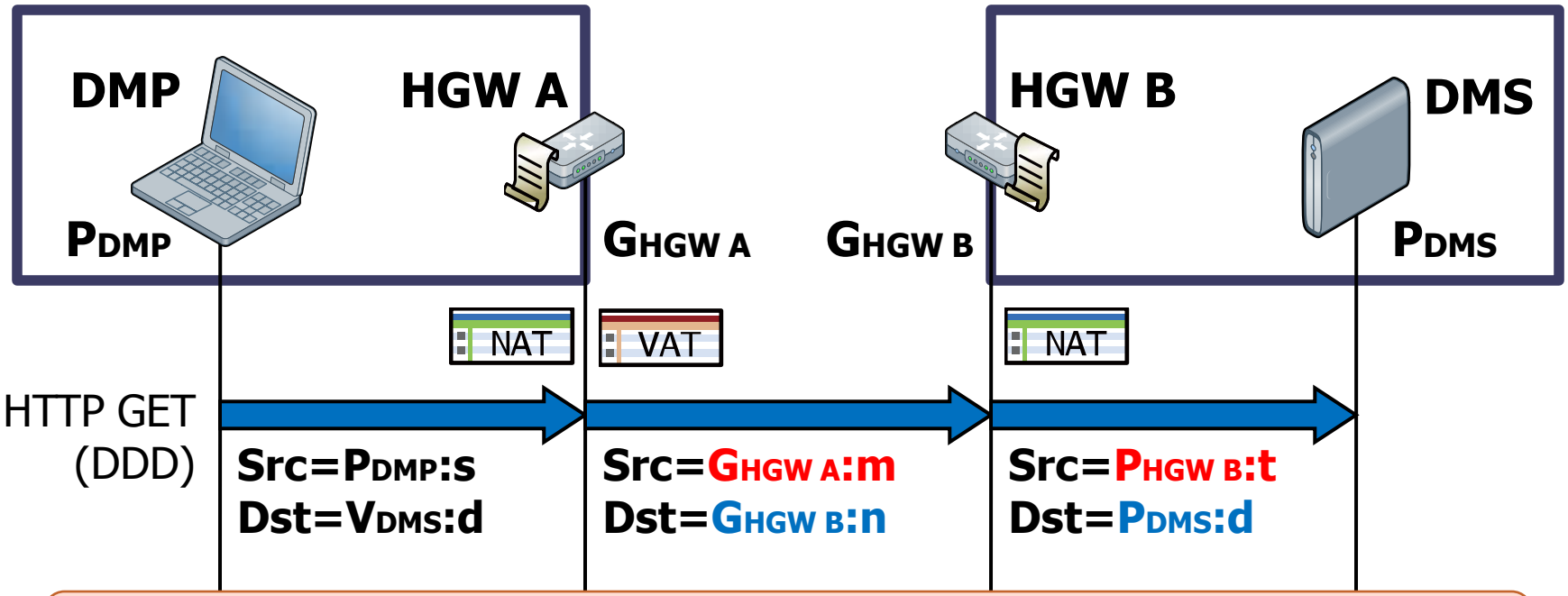
アドレス変換テーブルの詳細



送信元がHGW ➔ DMSは同一NWからのアクセスと認識

NAT越え通信

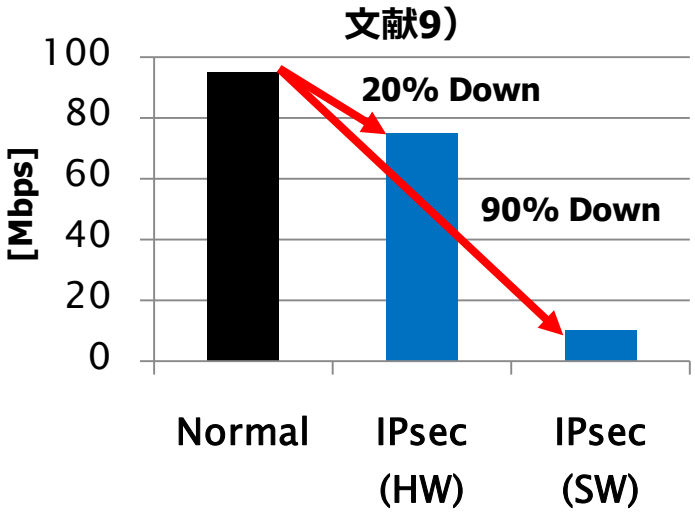
- 3回のアドレス変換処理を実行
  - HGW A： NAT（**送信元**），VAT（**宛先**）
  - HGW B： NAT（**送信元**+**宛先**）

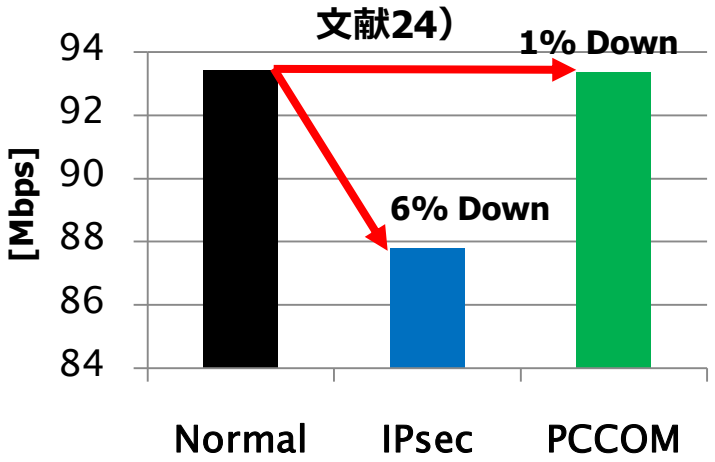


応答は逆の変換を実行 ➔ DMPとDMSの通信が成立

提案方式の特徴

- 既存技術と比較して**包括的なNAT越え通信**が可能
- コンテンツ伝送時のセキュリティ
  - PCCOM（Practical Cipher Communication）[24]
    ➔既存技術（IPsecを採用）より**高スループット**





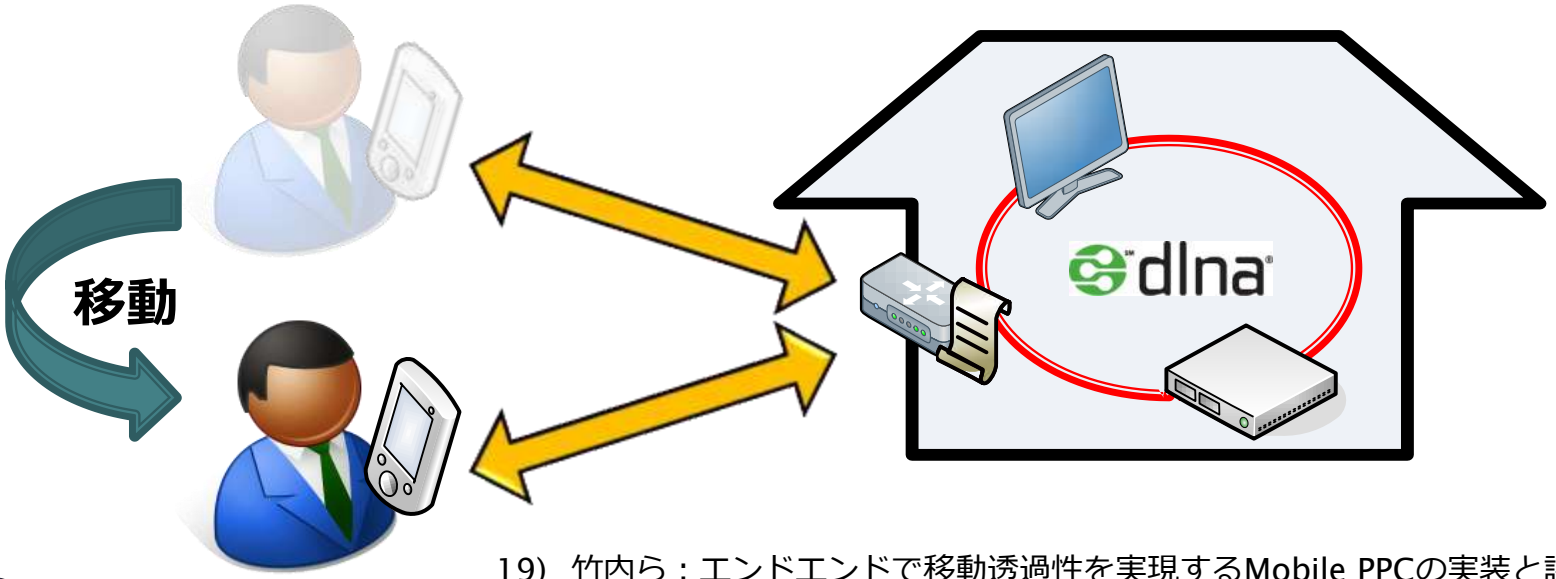
9) Jung-Tae Kim, et al. : Implementation of the DLNA Proxy System for Sharing Home Media Contents, IEEE Trans. Consum. Electron., Vol.53, No.1, pp.139-144 (2007)

24) 増田ら：NATやファイアウォールと共存できる暗号通信方式PCCOMの提案と実装，情処学論，Vol.47，No.7，pp.2258-2266 (2006)

提案方式の特徴

- モバイル機器も同様の仕組みを適用可能
  - さらに**移動透過性**もサポート可能
    - **Mobile PPC（Mobile Peer-to-Peer Communication）** 19)

      ➔通信中に移動しても，通信を継続
      （NAT-fとMobile PPCを組み合わせたシステムは実証済み20) ）



19) 竹内ら：エンドエンドで移動透過性を実現するMobile PPCの実装と評価，情処学論，Vol.47，No.12，pp.3244-3257 (2006)
20) 鈴木ら：NAT-fの移動透過通信への拡張，DICOMO2007，pp.857-865 (2007)

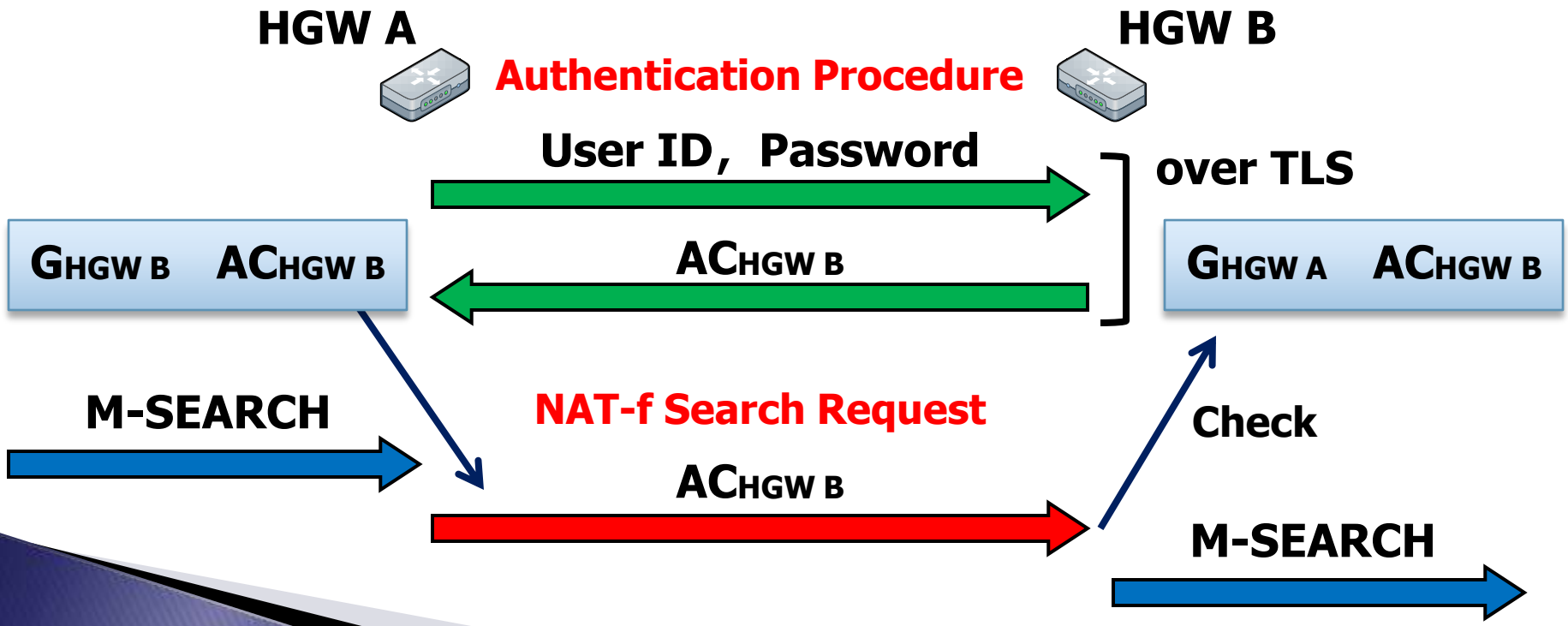
まとめ

- ホームネットワーク間のDLNA情報家電の相互接続方式を提案
  - 既存のNAT-fにDLNAサポート機能を追加
    - ホームネットワーク内の全ての機器と通信可能
  - モバイル機器にも対応
    - 移動透過性技術との組み合わせが可能
- 今後の課題
  - 通信開始時におけるユーザ認証手続き
  - 提案方式の実装と動作検証

付録

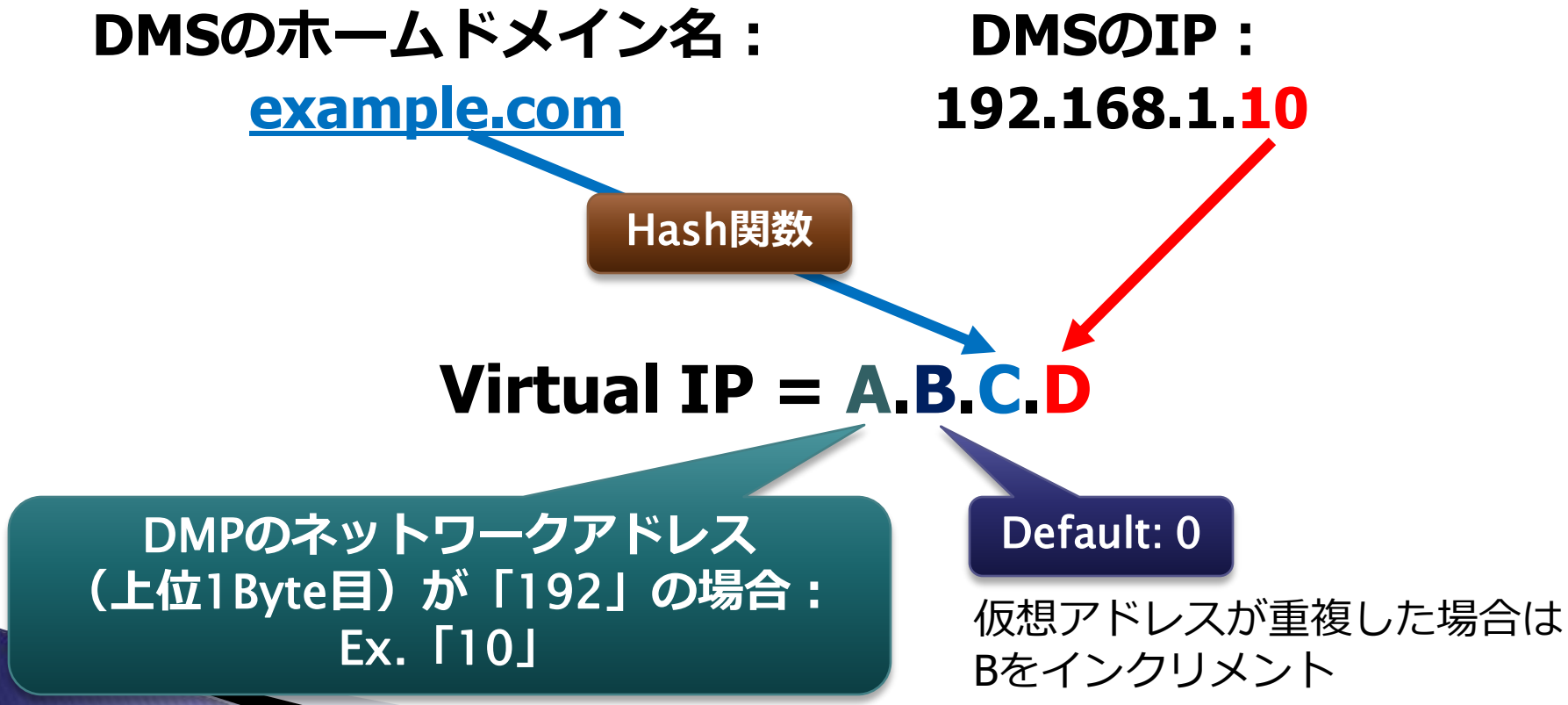
ユーザ認証手続き

- HGW Bに対してユーザ認証（TLSで通信を保護）
  - 認証成功➔ランダムなアクセスコードを生成し，HGW Aに返信
  - アクセスコードはSearch Request時に利用



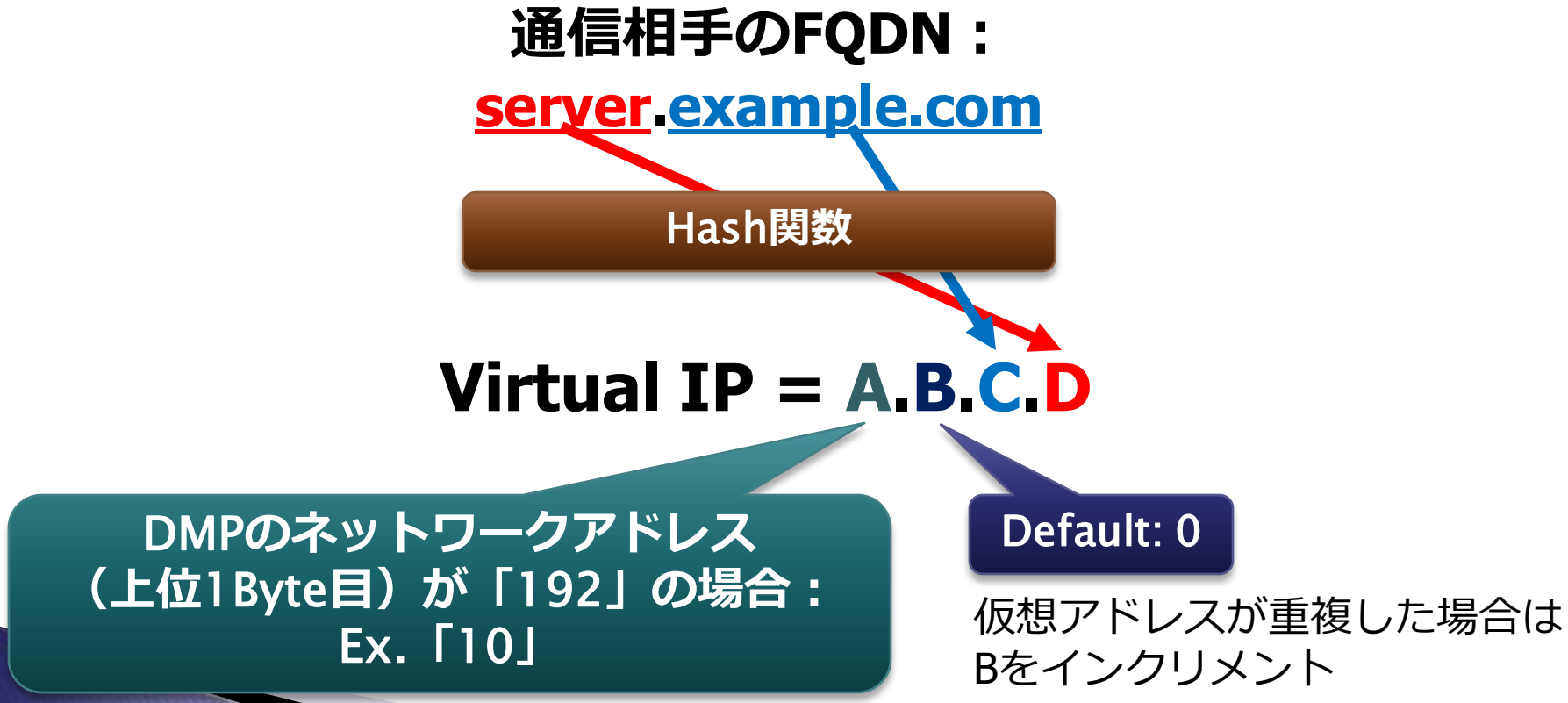
仮想IPアドレスの生成法

- DMSのホームドメイン名とDMSのホストアドレス
  - 上位1Byte目はDMPのネットワークアドレスと異なるプライベートアドレス



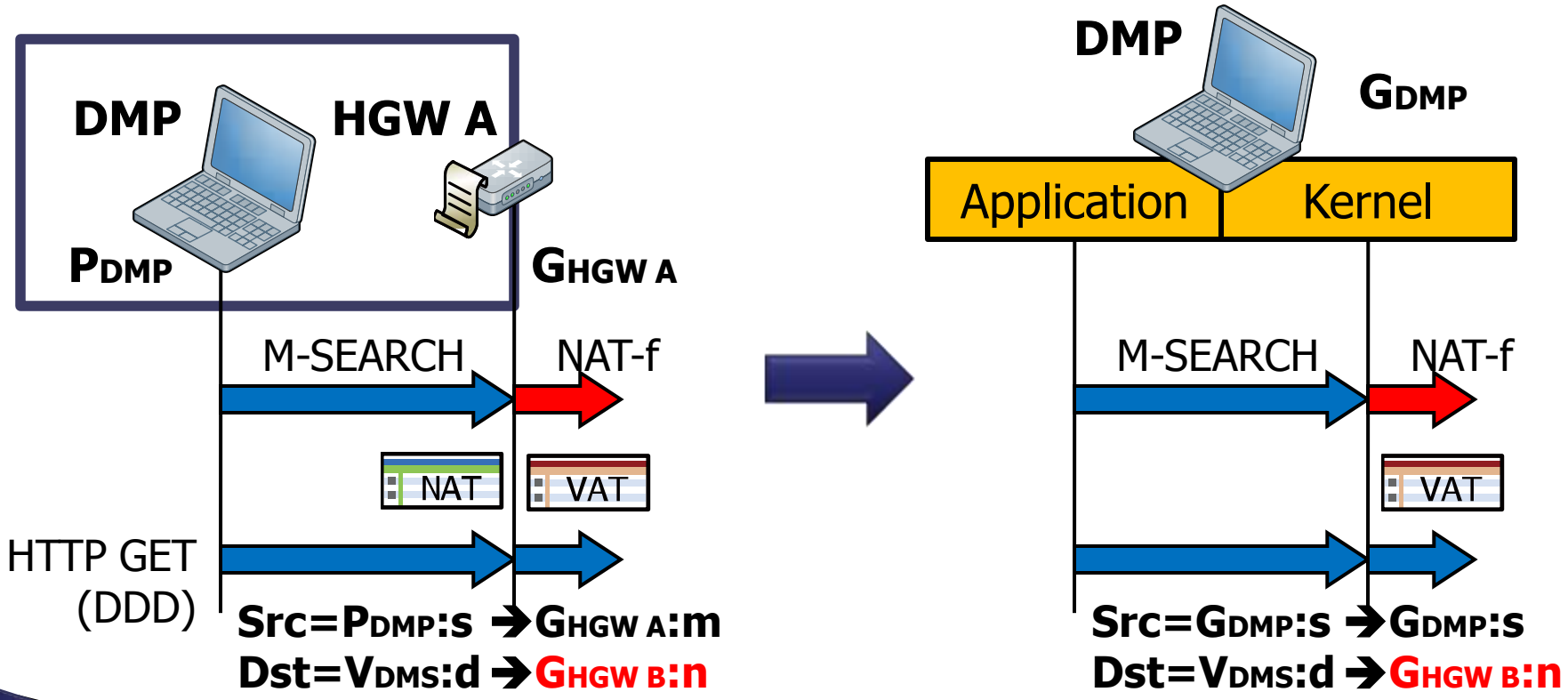
仮想IPアドレスの生成法（従来方式）

- 通信相手のFQDN
  - 上位1Byte目は通信開始端末のネットワークアドレスと異なるプライベートアドレス



モバイル機器への適用

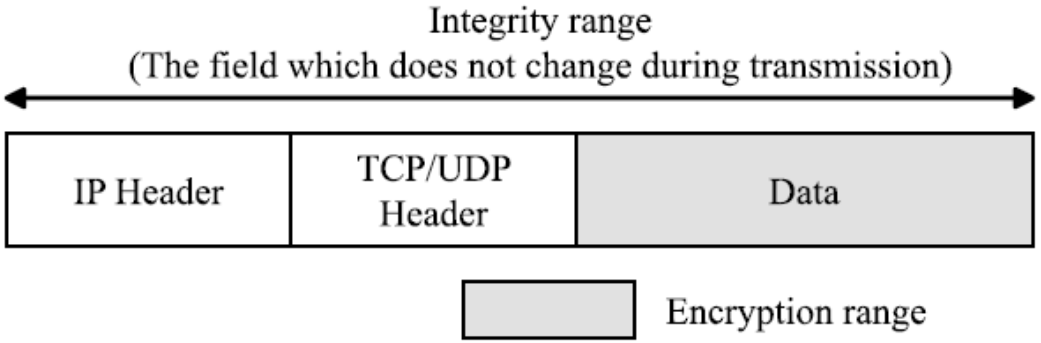
- Home-to-Homeの仕組みをそのまま適用
  - HGWのNAT-f機能をDMPのカーネルに実装



PCCOM（Practical Cipher Communication）

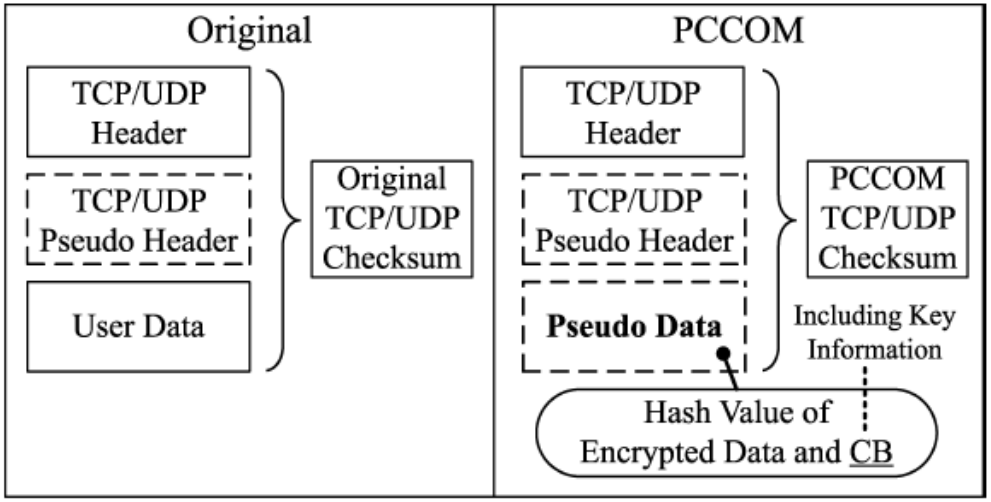
Watanabe Lab.

- NAT/FWを通過できる暗号化通信



パケットフォーマットを変えないまま本人性認証とパケットの完全性を保証

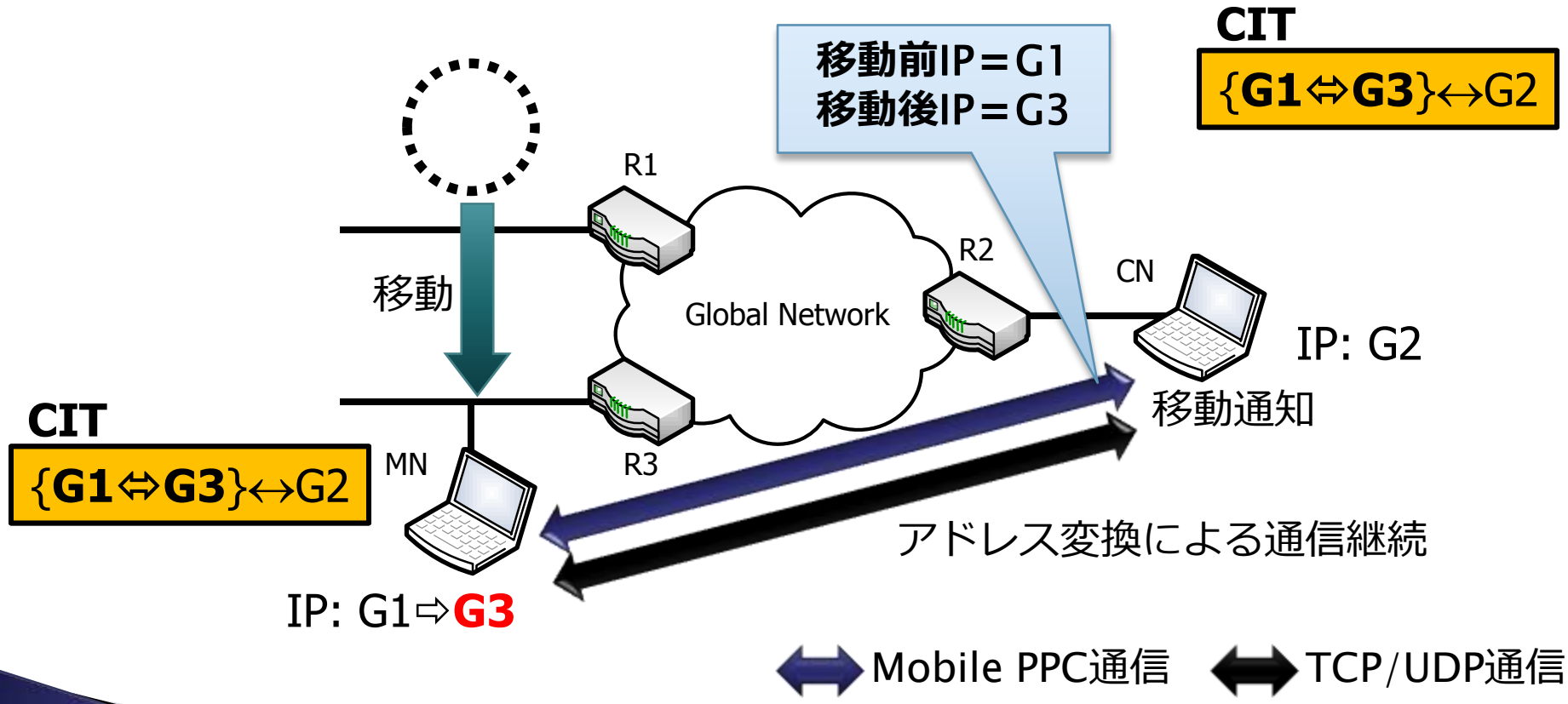
- 共通秘密鍵とパケットのIP・TCP/UDPヘッダで転送中に変化しないフィールドから，CB（Checksum Base）を生成



24) 増田ら：NATやファイアウォールと共存できる暗号通信方式PCCOMの提案と実装，情処学論，Vol.47，No.7，pp.2258-2266 (2006)

Mobile PPC

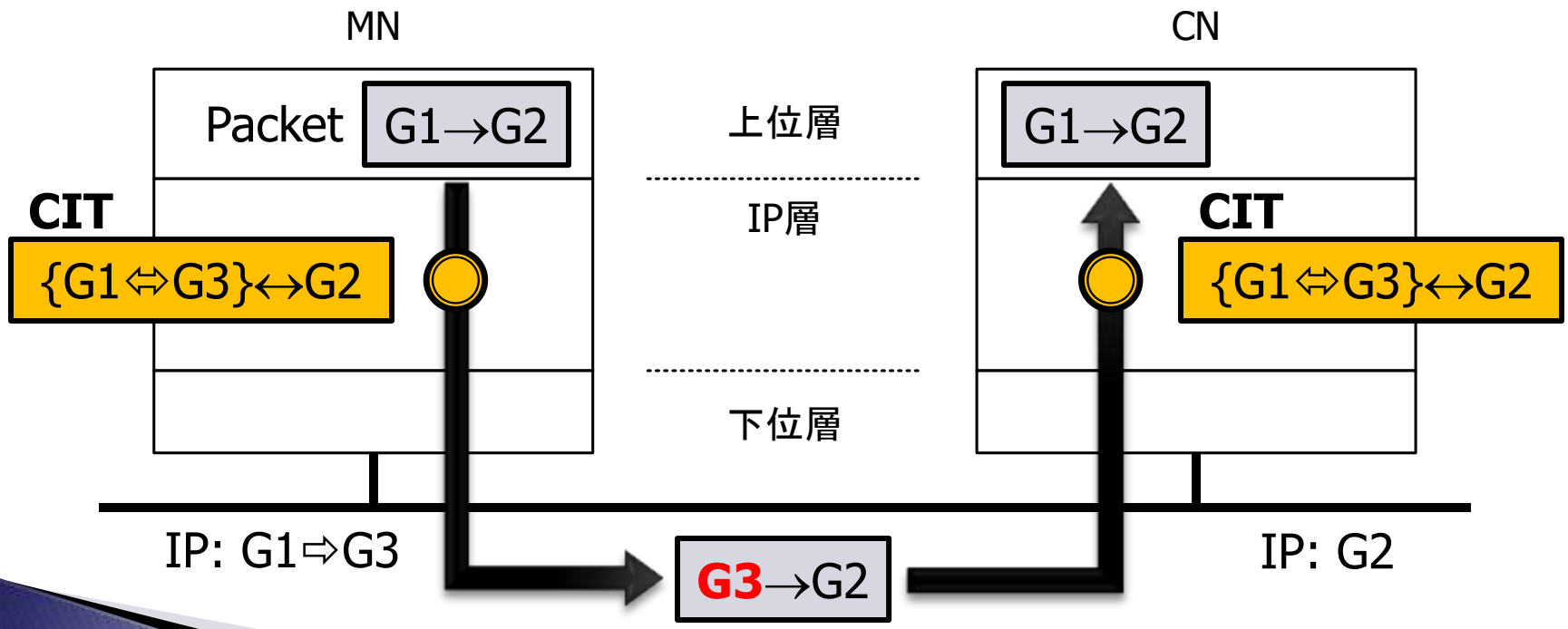
- 移動後にアドレスの変化を通知
  - アドレス変換テーブルCITを作成（更新）



19) 竹内ら：エンドエンドで移動透過性を実現するMobile PPCの実装と評価，情処学論，Vol.47，No.12，pp.3244-3257 (2006)

Mobile PPC

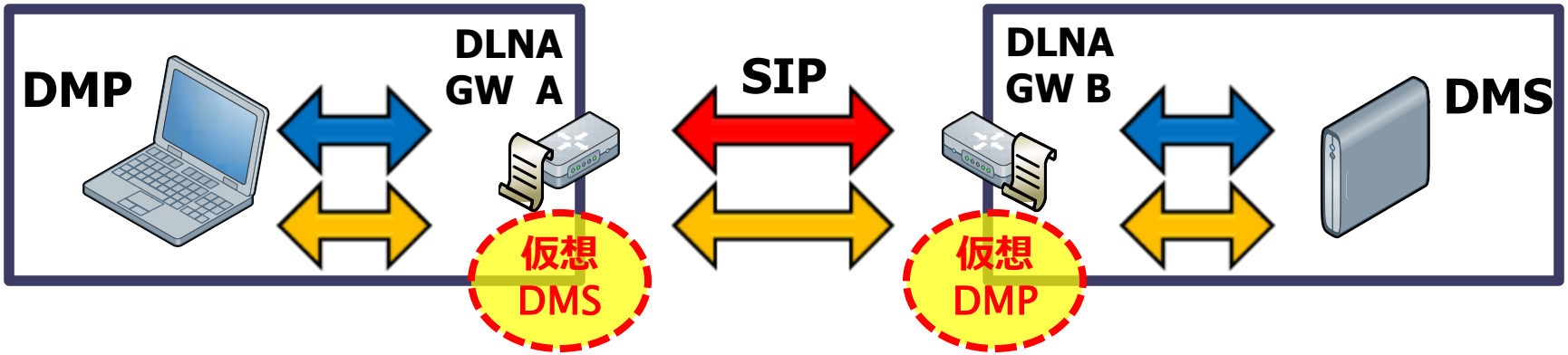
- CITに基づいたアドレス変換により通信を継続
  - 上位層：移動前のIPアドレスで認識
  - 下位層：移動後のIPアドレスでルーティング



既存技術

- デバイス検索の補完方法としてSIPを利用する技術
  - W-DLNA
    - ゲートウェイ内に仮想的なDMS，DMPプロセスを生成

    ➔通信相手が同一ホームネットワーク内にいると認識
    - デバイス検索のメッセージ交換にSIPを利用



  - Wormhole Device
  - 拡張DLNAメディア共有システムアーキテクチャ

既存技術

- VPNを構築する技術
  - Dial-to-Connect VPNシステム
  - DLNA Proxyシステム

- WWWサービス化
  - モバイルGWによりDLNAからのXMLをHTTPに変換

  ➔DMP側端末はWWWブラウザによりコンテンツを再生

- UPnPメッセージをカプセル化して転送
- xUPnP
  - 拡張UPnPアーキテクチャ（Peer-to-Peerを想定）

既存技術との比較

Watanabe Lab.
Department of Information Engineering, Meijo University
Information Networks Laboratory

表 2　既存技術との比較
Table 2　Comparison with existing technologies.

比較項目	W-DLNA	WD/Mobile-WD	D2C VPN	DPS	提案方式
遠隔地のデバイス検索を実現する補完技術	SIP	SIP	VPN	VPN	NAT-f
メディア伝送の NAT 越え実現手法	NAT マッピング	UPnP	VPN	VPN	NAT-f
セキュリティ（ユーザ認証時）	SIP (TLS)	SIP (TLS)	SIP (TLS)	IPsec ESP	TLS
セキュリティ（メディア伝送時）	×	× (IPsec ESP *1)	IPsec ESP	IPsec ESP	PCCOM
高スループットの維持	○	○ (×*1)	△	×	○
非 DLNA 機器に対する通信のサポート	×	×	○	○	○
モバイル機器のサポート	○	○	×	○	○
モバイル機器における移動透過性のサポート	×	×	×	×	○
ホームゲートウェイの変更	× 必要	○ 不要	× 必要	△*2	× 必要

WD: Wormhole Device[6)]　D2C VPN: Dial-to-Connect VPN System[11)]　DPS: DLNA Proxy System[9)]
*1 WD 間における VPN 適用時　*2 VPN 非対応の場合は変更が必要