

## VPN を介した情報家電サービス利用方式の提案

春山 敬宏<sup>†</sup> 水野 伸太郎<sup>†</sup> 山田 孝二<sup>†</sup> 水野 修<sup>†</sup>

<sup>†</sup> NTT 情報流通プラットフォーム研究所

本論文では、家庭内 LAN でのみ行われていた UPnP や DLNA によるプラグアンドプレイを遠隔の家電やサーバとも行えるようにする、情報家電遠隔連携サービスを提案する。同様のサービスを実現するための関連研究として、VPN トンネリング方式や UPnP プロキシ方式が提案されているが、それらは VPN やプロキシ接続前の認証を PC 上でのユーザ情報登録などで行っており、実際に接続する家電端末上での認証方式を検討していなかった。そこで、我々は家電の DLNA クライアントソフトウェアのユーザインタフェースで簡単に行え、かつ外出先の LAN から自宅の LAN に接続する場合でも携帯電話を使って安全に行える認証方式を明らかにし、それを実装したシステム上で方式の確認を行った。

## Authentication for On-line Services using DLNA Client Interface on Home Appliances

Takahiro HARUYAMA<sup>†</sup> Shintaro MIZUNO<sup>†</sup> Kohji YAMADA<sup>†</sup> Osamu MIZUNO<sup>†</sup>

<sup>†</sup> NTT Information Sharing Platform Laboratories

We propose an authentication method that can be used through a content viewing interface such as the DLNA client on home appliances. Services that connect digital home appliances to another home LANs or to the servers over the Internet using VPN or UPnP proxies has recently been proposed, but an user authentication for these services still require users to operate computers to send their identities. Our method does not require users to input any information on the appliances and thus can be easily used over the DLNA client and provides consistent interface for home appliance users. Moreover, since we use a mobile phone to authenticate users, it is safe to be used even in the remote location. We show operations of the method using a simple prototype system.

### 1 はじめに

ネットワーク機能を持つ家電、いわゆる情報家電が普及しており、2009 年には HDD/DVD レコーダやデジタル TV などを中心とした情報家電が、PC を出荷台数において上回ると予想されている [1]。現在でも、ロケーションフリー [2] によるコンテンツの遠隔視聴サービスが、ニーズの高いサービスとして注目を集めている。このサービスは自宅に保存してあるコンテンツを、事前に登録してあるポータブルな機器（ノート PC やゲーム機など）を使って遠隔から試聴するものである。

また、家庭内の LAN においては、UPnP (Universal Plug and Play) フォーラム [3] や DLNA (Digital Living Network Alliance) [4] が策定している家電連携のプロトコルが普及しつつある。UPnP は、新しく家庭内 LAN に接続する家電が、特別な設定をしなくても LAN 内の他の家電を自動的に発見して登録する連携機能を規定している。UPnP を活用する DLNA に準拠した家電製品は、徐々に市販されてきており [5] [6] [7]、対応製品は今後ますます増えていくと思われる。

将来、UPnP や DLNA が策定するプロトコルは、情

報家電ユーザに利便性の高いネットワークサービスを提供するための標準プロトコルになり、家庭内 LAN の機器にあるコンテンツを試聴するのみでなく、遠隔の機器のコンテンツを試聴する際にも利用されるようになることが予想される。本論文では、いつでもどこでも情報家電を使って、遠隔から自宅や集中サーバにあるコンテンツを試聴したりすることを目的とした、情報家電のサービス利用方式について認証方式を中心に提案する。

### 2 情報家電遠隔連携サービスの提案

#### 2.1 情報家電遠隔連携サービスの概要

情報家電を使って遠隔のコンテンツを簡単に試聴できるためのサービスとして、情報家電遠隔連携サービスを提案する。情報家電遠隔連携サービスは、従来、UPnP や DLNA を用いて家庭内 LAN の家電間でのみ行われていた家電連携を、別の家庭内 LAN につながれている家電や、サービスプロバイダが提供するサーバとも行えるようにするサービスである。

このサービスでは、ユーザは家庭内の機器に接続す

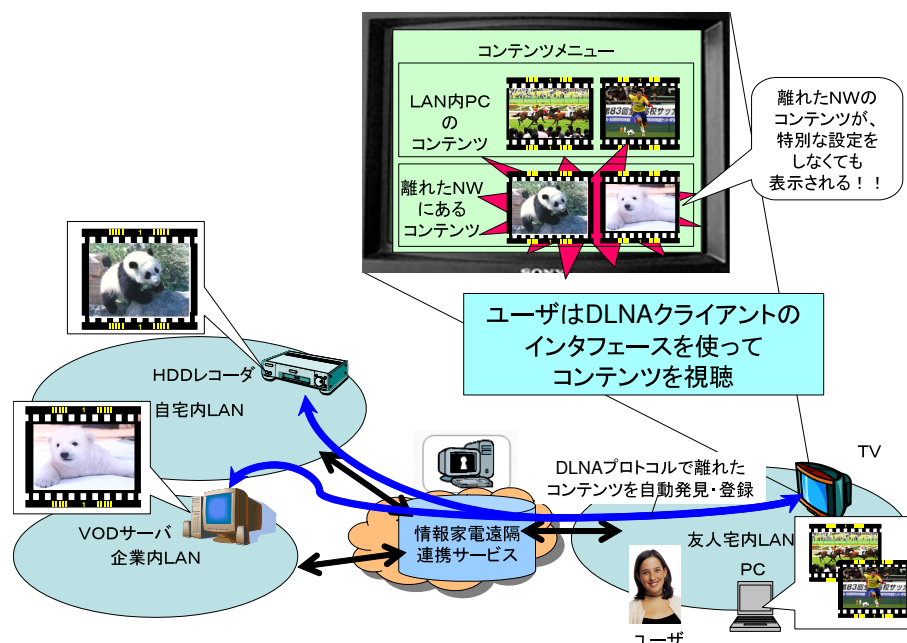


図 1 情報家電遠隔連携サービス

るのと同じ様に、機器やコンテンツの選択・再生などの機能を提供する DLNA のクライアントソフトウェアをサービスのインターフェースとして使用する。その結果、ユーザは家庭内でコンテンツを試聴するのと同等の簡易さで、遠隔地からでもコンテンツの試聴ができるようになる。

## 2.2 提案サービスのユースケース

本サービスの具体的なユースケースについて説明する。

### (1) ユーザが自宅のコンテンツを遠隔から視聴するサービス

図 1 は、友人宅にいるユーザが、自宅にある HDD レコーダに蓄積されている映像コンテンツを友人宅の TV から視聴する利用シーンが示されている。

具体的には、友人宅 LAN 内の TV が自宅 LAN 内の HDD レコーダを自動的に発見して、蓄積されたコンテンツに関する情報を登録する。ユーザは、TV のコンテンツメニュー画面を更新させるだけで、自宅 HDD レコーダのコンテンツを表示させて視聴することが可能になる。

このサービスによって、ユーザは自宅で HDD レコーダのコンテンツを DLNA のプロトコルを使って自動的に検索して視聴するのと同じ簡単さで、遠隔視聴を行うことができる。

### (2) プラグアンドプレイによる VOD サービス

家庭内 LAN にある家電が、コンテンツ配信サーバと連携した場合に実現できる VOD サービスについて説明する。このユースケースでは、LAN 内にある端末もしくは家庭内 LAN の入口となるホームゲートウェイ (以下 HGW) が、DLNA による家庭 LAN 内の機器のコンテンツ検索要求を、遠隔のサービスプロバイダのサーバに転送する。家庭内 LAN の家電はサービスプロバイダが設置するサーバを自動的に発見して、サーバの提供するコンテンツ情報を登録する。このサービスによってユーザは、UPnP や DLNA のプロトコルに対応している情報家電であれば、機器毎にセットトップボックスを接続したり、事前にサービスのための設定をする必要がなくなる。

## 2.3 提案サービスに関連する従来研究

前述したユースケースを実現する技術として、LAN 内のみ有効であった家電連携のプロトコルのパケットを、遠隔のネットワーク間で転送する接続技術がある。

従来研究 [8] では、UPnP プロトコルをプロキシもしくは VPN でトンネリングする機能を、HGW に配備する方式を検討している。また、従来研究 [9] の実証実験は、HGW 間で DLNA プロトコルをプロキシすることで、遠隔のネットワークにある家電のコンテンツを、DLNA クライアントから試聴できるようにしている。

しかしながら、これら 2 つの従来研究においては、ゲートウェイ間で家電連携プロトコルをプロキシで転送するもしくは VPN でトンネリングする接続方式に主眼が置かれており、接続を確立する前に必要となる認証について、十分に検討がされていない。従来研究 [8] は、PC を使って許可する家電を登録しておくやり方をとっている。

本論文では、外出先の家電端末を使用するユーザが、自宅にあるコンテンツや企業の VOD サーバが提供するコンテンツを、DLNA のプロトコルを用いて簡単に視聴するサービスを受ける際に、必要な認証技術についての検討を行う。

### 3 提案サービスに向けた認証技術の検討

#### 3.1 要求条件

提案サービス実現のための要求条件を以下に示す。

要求条件 1：モビリティを確保すること

提案サービスでは、外出先の任意の端末で認証を受けるユースケースを主に想定している。よって、認証を受ける家電に対して、証明書などの認証情報を事前に配布し、それによる機器認証を実行するという方式は使えない。そのため、どこにある機器からでもサービス利用の都度ユーザを認証できるようなモビリティを確保した認証方式が必要である。しかしながら、外出先の家電に、ID・パスワード情報を入力することは、キーロガーやパケットの盗聴などによる盗難のリスクが高い。よって、どこでも安全に認証でき、認証情報の盗難に耐性のある方式が要求される。

要求条件 2：DLNA のインタフェースを使って認証が完結すること

提案する遠隔コンテンツ視聴サービスを利用する際、DLNA クライアントのインタフェースを用いる。このインタフェースは、コンテンツを蓄積している機器やコンテンツの選択・再生などの画面ボタンがなく、またウェブブラウザのように認証のためのアクセス手段や情報入力フォームも存在しない。このようなインタフェースにおいて、従来の認証方式である ID・パスワード方式を、適用することは困難である。

これらの要求条件 1，2 から、以下の 2 つの課題について検討する必要がある。

- 外出先でも安全に認証できること
- DLNA クライアントソフトウェアのような認証情報の入力が困難なインタフェースにおいても認証できること

#### 3.2 検討方式

##### 3.2.1 外出先でも安全に認証できる方式

外出先の PC のウェブブラウザなどで、認証を安全に行う方式として、我々はこれまで携帯電話を利用したマルチチャンネル認証方式 [10] について検討を行ってきた。

マルチチャンネル認証方式について図 2 で説明する。まずユーザが PC ブラウザなどからサーバにアクセスすると、サーバは QR コードを、サーバの認証画面ページに表示する (フロー 1, 2)。QR コードには、URL やセッション情報と呼ばれる PC と携帯電話を関連づけるための情報が含まれる。セッション情報は、その認証セッション中のみ有効な一時的な情報であり、リクエストするユーザ毎に一意に割り当てられる。次にユーザは表示された QR コードを携帯電話のリーダを使って読み取り、携帯電話網経由で携帯電話に事前に保管している認証情報 (携帯電話の個体番号や証明書など) と一緒にサーバに送信する (フロー 3, 4)。認証サーバは認証情報をもとに携帯電話を所有するユーザを同定し、その上でセッション情報をもとに PC を使用するユーザのログインを許可する (フロー 5)。

マルチチャンネル認証方式は、盗聴のリスクが高い外出先のネットワーク経由で認証情報を送らずに、リスクがより低い携帯電話網経由で認証情報を送信する。その結果、信頼できない外出先の端末においてもユーザは、安全に認証を行いサービスを受けることが可能になる。また、一般に広く普及している携帯電話を利用するため、特殊なハードウェアが不要である。

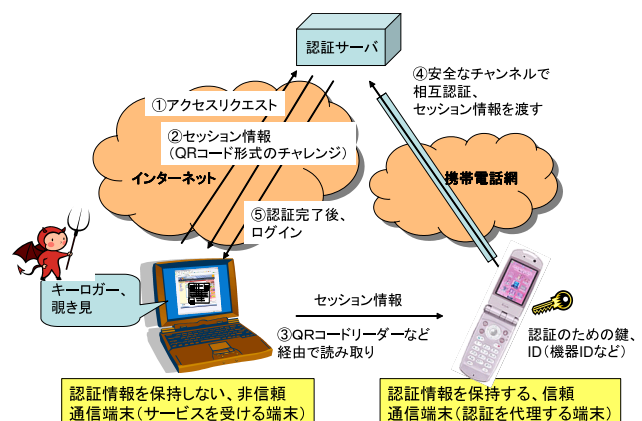


図 2 マルチチャンネル認証方式

### 3.2.2 入力が困難な IF においても認証できる方式

マルチチャンネル認証は，外出先でも安全に認証できる方式であるが，あくまで PC 端末等のウェブブラウザなどで用いることを想定している．提案サービスのよう DLNA クライアントソフトウェアのインタフェースを使って認証したい場合，セッション情報を表示するサーバへのアクセス手段が存在しなかった．

例えばウェブブラウザのブックマークのように，ボタンのクリックだけでサーバの認証画面を表示させる方法があれば，コンテンツの選択・再生の操作しかできないインタフェースでも簡単にマルチチャンネル認証を行うことができる．

そのため，我々は HGW がサーバにアクセスして取得した認証画面を，ユーザの家電画面に表示する方式を検討する．

### 3.3 DLNA クライアント向け携帯認証方式

本節では 3.2 節で述べた 2 つの検討方式を組み合わせた DLNA クライアント向け携帯認証方式を提案する．ここでは，ユーザが友人宅から自宅にアクセスするユースケースを例に説明する．

#### 3.3.1 システム構成

DLNA クライアント向け携帯認証方式を適用する情報家電遠隔連携サービスのシステム構成を図 3 に示す．情報家電遠隔連携サービスでは，DLNA に対応している家電であればサービスを受けられるように，HGW 同士の VPN 接続や DLNA プロキシ機能などによって，家電連携のパケットを転送する．

また，接続相手の IP アドレスや VPN に必要となる鍵などの接続情報を安全に共有するために，中継サーバを利用した接続を行う．中継サーバと HGW の間は，証明書の相互認証などによって安全な通信路が確立されている．

中継サーバは図 4 のように認証データベースと VPN 情報データベースを保持し，認証データベースにはユーザの ID，認証情報，セッション情報，HGW が携帯電話によって認証されたかどうかを示すフラグが含まれる．VPN 情報データベースにはユーザの ID に関連づけられた自宅 HGW の位置情報が含まれる．自宅 HGW の位置情報は，HGW のアドレスが変わるたびに HGW からの通知によって定期的に更新される．

#### 3.3.2 方式のフロー

DLNA クライアント向け携帯認証方式のフローについて，図 5 のフロー図を用いて説明する．

ユーザが友人宅の TV の DLNA クライアントから友

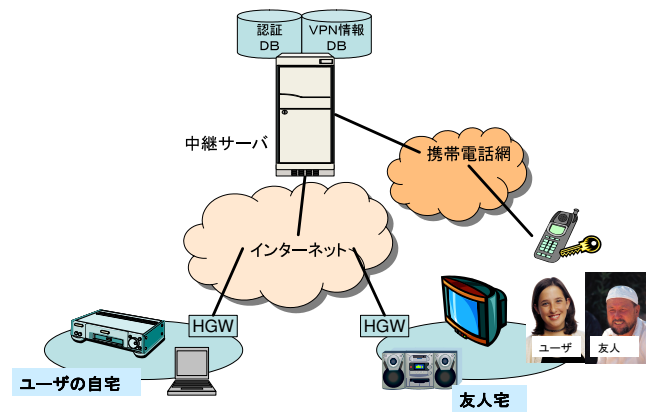


図 3 提案する認証方式におけるシステム構成

| 認証データベース |                     |           |               |
|----------|---------------------|-----------|---------------|
| ユーザID    | 認証情報(端末の<br>個人番号など) | セッション情報   | 認証終了済み<br>フラグ |
| haru     | serXXXX             | 12345678※ | True          |
| ⋮        | ⋮                   | ⋮         | ⋮             |

※セッション情報は一時的な情報

| VPN情報データベース |               |
|-------------|---------------|
| ユーザID       | 自宅HGWの位置情報    |
| haru        | 212.51.105.33 |
| ⋮           | ⋮             |

図 4 中継サーバが保持するデータベース

人宅の HGW にアクセスすると，QR コードを含む認証画面が表示される（フロー 1）．その後，友人宅の HGW が，携帯電話による認証が終了したかどうかを中継サーバに問い合わせる（フロー 2）．

ユーザは，表示された認証画面に埋め込まれた QR コードを携帯電話のリーダーで読み取り，読み取ったサーバの URL に携帯電話に保存された認証情報とセッション情報を送る（フロー 3，4）．

認証が終了すると，友人宅 HGW 側のポーリングも終了し，中継サーバはデータベースから取得した位置情報などを友人宅 HGW と自宅 HGW の両方に送信する（フロー 5-7）．その後，双方の HGW がエンドツーエンドで VPN の接続を行い，中継サーバから携帯電話に接続が成功したことが伝えられる（フロー 8，9）．

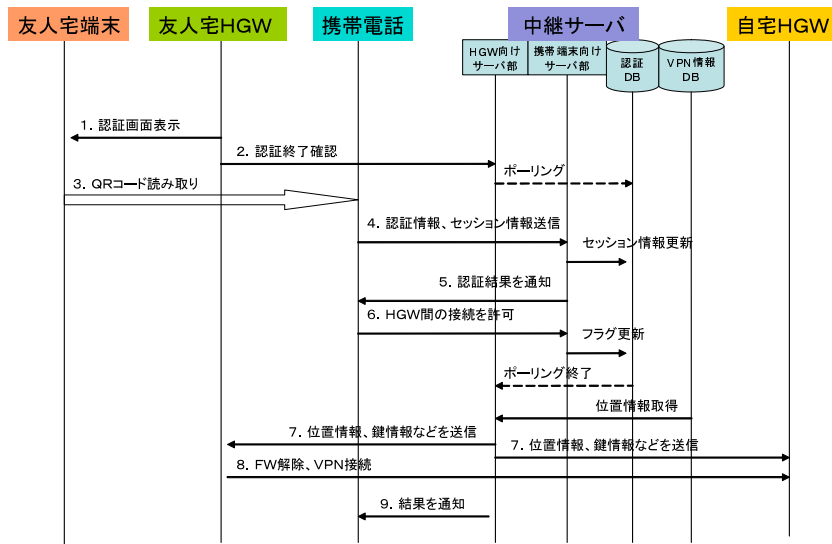


図 5 提案方式のフロー

### 3.3.3 実装

方式の実現性を確認するため、DLNA クライアント向け携帯認証方式から情報家電遠隔連携サービスを利用するシステムについて、HGW と中継サーバに必要なとなるソフトウェアを、それぞれ PC 上に実装した。以下、実装システムの画面について説明する。なお、実装では、DLNA クライアントソフトウェアとして市販の製品 [11] を、認証後に構築する DLNA プロトコルを転送する VPN のソフトウェアとして OpenVPN [12] を使用している。



図 6 友人宅 HGW による認証画面の表示

図 6 は、友人宅 HGW によって表示された QR コードを含む認証画面である。

図 7 では、ユーザは携帯電話の QR コードリーダーから表示された QR コードの情報を読み取っている。

QR コードで読み込んだ URL からサーバにアクセス



図 7 認証画面における QR コード読み取り

すると、図 8 の画面が現れ、ユーザはボタンを押して認証情報を送る。認証終了後、HGW 間で VPN 接続が行われる。

VPN 接続後、ユーザが DLNA クライアントにおいてコンテンツを検索すると、離れた自宅のコンテンツサーバ機器が図 9 のように現れる。そして、ユーザは図 10 の画面において、自宅のコンテンツを選択して試聴することができる。

実装システムから、以下の 2 点が明らかになった。

- DLNA クライアントのように、ウェブブラウザのようなアプリケーションでなくても認証画面を表示できること

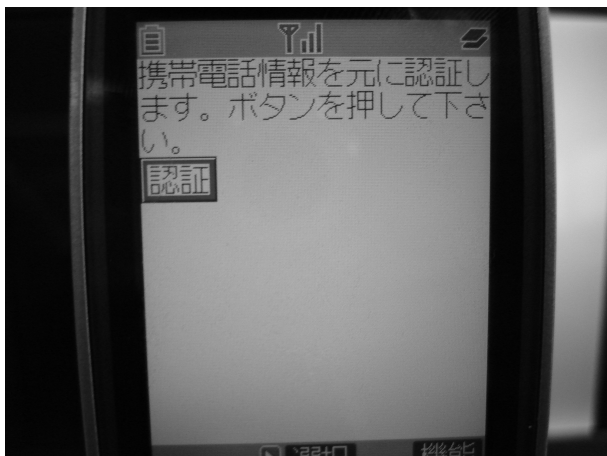


図 8 携帯電話での認証

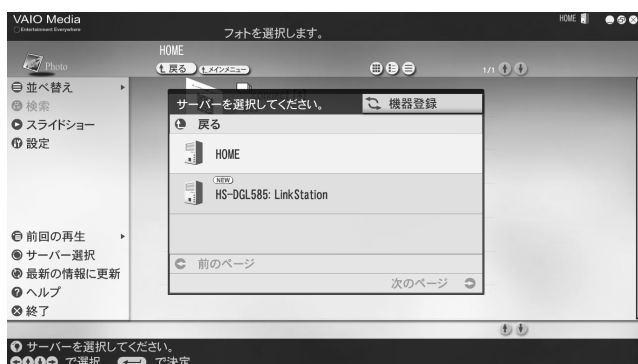


図 9 自宅のコンテンツサーバを検索

- マルチチャンネル認証が、市販の DLNA クライアントソフトウェアのインタフェースに対しても適用可能であること

これらの結果により、DLNA クライアント向け携帯認証方式は、外出先でも安全に認証できかつ DLNA クライアントソフトウェアのユーザインタフェースでも簡単に行える認証方式であり、3.1 節で述べた要求条件を満たすことを確認できた。

#### 4 まとめ

本論文では、家庭内 LAN でのみ行われていたプラグアンドプレイによる家電連携を、遠隔の家電やサーバとも行う情報家電遠隔連携サービスを提案した。また、そのサービスを行うにあたって必要となる VPN 接続またはプロキシ接続を確立する前の認証方式について検討し、その方式を実装により確認した。

今後は、ユーザが自宅から別の友人宅の LAN に接続して友人宅のコンテンツを遠隔から試聴するユースケースについても検討していく予定である。



図 10 自宅コンテンツの選択

#### 参考文献

- 1) 株式会社野村総合研究所. 2009 年までの国内 IT 主要市場の規模とトレンドを展望, 2005. <http://www.nri.co.jp/news/2005/050114.html>.
- 2) ソニー株式会社. Locationfree「ロケーションフリー」. <http://www.sony.jp/products/Consumer/locationfree/index.html>.
- 3) The UPnP™ Forum. <http://www.upnp.org/>.
- 4) Digital Living Network Alliance. <http://www.dlna.org/industry/home-jp/>.
- 5) 株式会社東芝. 東芝 LZ150 シリーズ「DLNA ガイドライン対応」機能アップグレードについて, 2005. <http://www.toshiba.co.jp/product/tv/info/050418.htm>.
- 6) 株式会社東芝. 東芝 HDD&DVD レコーダー新商品の発売について, 2006. [http://www.toshiba.co.jp/about/press/2006\\_01/pr-j1701.htm](http://www.toshiba.co.jp/about/press/2006_01/pr-j1701.htm).
- 7) ソニー株式会社. ソニー ブラビア X シリーズ DLNA 対応機器リスト, 2005. <http://www.sony.jp/products/Consumer/bravia/support/dlna.html>.
- 8) 森谷高明, 大西浩行, 吉田誠, 小川猛志, 伊藤匡. ホームネットワーク内の情報家電機器へのリモートアクセス方式に関する一検討. 電子情報通信学会 2006 総合大会, 2006.
- 9) モバイル・ホームシステム協議会. 情報家電ネットワーク相互接続技術の実証実験 プレスリリース, 2005. <http://mhsf.jeita.or.jp/jikkenn/pressrelease/2005-12-19.pdf>.
- 10) Shintaro Mizuno, Kohji Yamada, and Kenji Takahashi. Authentication using multiple communication channels. In *ACM Workshop On Digital Identity Management*, pp. 54–62, 2005.
- 11) ソニー株式会社. VAIO — VAIO Media. <http://www.vaio.sony.co.jp/Products/Solution/VAIOMedia/>.
- 12) James Yonan. OpenVPN - An Open Source SSL VPN Solution by James Yonan. <http://openvpn.net/>.