

# ネット家電の標準化技術の現状と展望

Current Status of and Future Prospects for Standardization of Network Home Appliances

神田 充 寺島 芳樹 安次富 大介

■ KANDA Mitsuru

■ TERASHIMA Yoshiki

■ AJITOMI Daisuke

近年、ネットワーク接続機能を装備したAV機器や白物家電が登場してきている。しかし、ホームネットワークにおけるネット家電の通信方法には多くの規格が存在し、相互接続性の問題が生じている。また、インターネットを介して通信する場合、通信の安全性が求められている。

東芝は、これらネット家電の普及のうえで障害となる問題を解決するため、ホームネットワーク内の通信の相互接続性を改善する技術となるECHONET-UPnP (Universal Plug and Play) ゲートウェイと、インターネットを介した安全な通信を実現する技術となるUOPF (Ubiquitous Open Platform Forum) の規格化に貢献した。これらを組み合わせることによりネット家電間の相互接続性を向上させ、インターネットを介した安全な通信を実現することが可能になる。

An increasing number of network home appliances, namely, network-connected white goods and audiovisual (AV) devices, have entered the consumer market in recent years. However, technical difficulties related to interconnectivity may sometimes be encountered because so many standards are provided for network home appliances. In addition, networking needs to be confirmed as safe when network communication is established. These issues can be stumbling blocks to the dissemination of network home appliances.

Toshiba has contributed two technologies to the development of network home appliances: the "ECHONET-universal plug and play (UPnP) gateway" to improve the interconnectivity of network home appliances, and the "ubiquitous open platform forum (UOPF)" to offer safe networking for network communication. These two technologies work cooperatively for the realization of consumer-friendly network home appliances.

## 1 まえがき

インターネットへのブロードバンド常時接続が一般家庭にも普及して、ネット家電と呼ばれる通信機能を持ったAV機器や白物家電などが登場してきている。しかし、ホームネットワークにおけるネット家電間の通信方法には多くの規格が存在しているため、相互接続性の問題が生じ、ネット家電向けアプリケーション開発の障害となっている。また、インターネットを介して通信する場合には、安全性の確保が求められている。

ここでは、ホームネットワークにおけるネット家電の相互接続性を改善するための技術となる“ECHONET-UPnP (Universal Plug and Play) ゲートウェイ”と、ネット家電がインターネットを介して簡単に安全に通信するための技術となる“UOPF (Ubiquitous Open Platform Forum)”について述べる。

## 2 ECHONET-UPnP ゲートウェイ

ホームネットワークにおけるネット家電制御プロトコルの標準規格として、UPnPやECHONETなどが挙げられる。AV機器や白物家電の統合的な管理・操作サービス実現のため

には、ユーザーやサービス提供者が、これら種々のネットワークプロトコルの違いを意識することなく扱えるよう(透過的)になるのが望ましい。この章では、UPnPとECHONETとを透過的に扱うための技術であるECHONET-UPnPゲートウェイについて説明する。

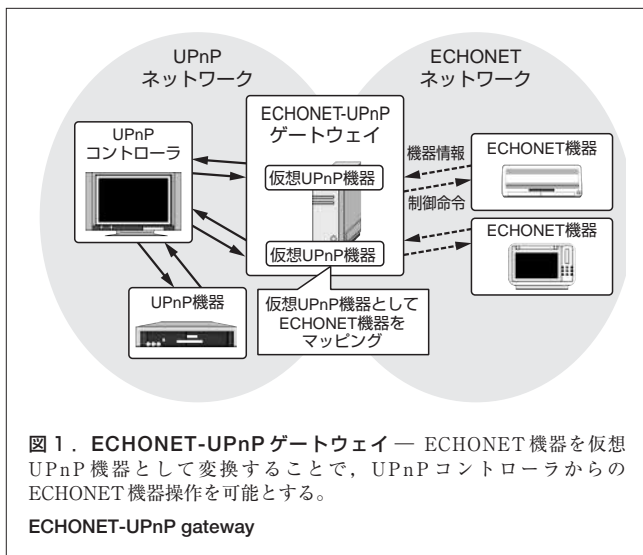
### 2.1 ECHONET-UPnP ゲートウェイ技術

UPnPは、マイクロソフト社が中心となって提唱したネット家電制御プロトコルであり、主にパソコン(PC)やAV機器に広く採用されてきている。一方ECHONETは、国内家電メーカー中心の団体であるエコーネットコンソーシアムによって策定された、白物家電向けのネット家電制御プロトコルである。

ECHONET-UPnPゲートウェイは、PCやAV機器などを扱うUPnPと、白物家電を主に扱うECHONETとの間の連携・仲介機能を提供する(図1)。この機能により、テレビなどのUPnPコントローラ(操作端末)は、通常のUPnP機器だけでなく、ECHONET機器をも仮想的なUPnP機器として認識し、制御することが可能となる。

### 2.2 ECHONETとUPnPのマッピング方法

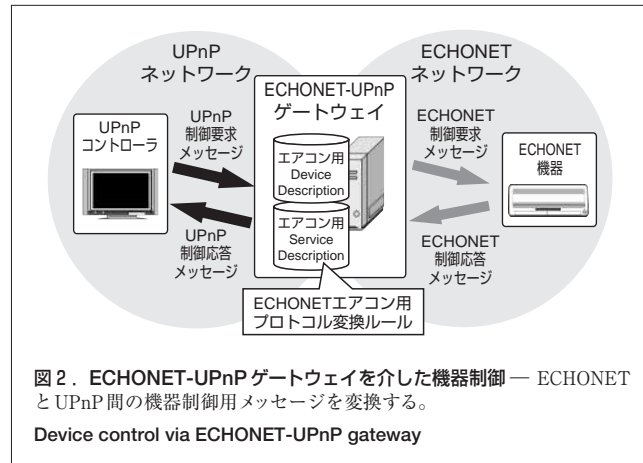
UPnPは、Discovery(機器の参入通知)、Description(機器情報の提供)、Control(機器の制御)、Eventing(機器からの通知の検出)といった機器操作のための動作ステップを



各々定義している。

ECHONET-UPnP ゲートウェイは、UPnP での各動作ステップに対応する機能を、ECHONET によって実現し、UPnP にマッピングさせることで、ECHONET 機器を仮想的な UPnP 機器として扱えるようにする。以下にマッピング方法の概要を示す。

- (1) **Discovery** ゲートウェイは、ECHONET 機器からのマルチキャストによる参入通知を検出すると、1 台の仮想 UPnP 機器に相当する処理プロセスを開始し、UPnP による参入通知を発行する。また、検出した ECHONET 機器のアドレスを、UPnP のアドレスに一意に対応付ける。
- (2) **Description** ECHONET では、ECHONET Object Code (EOJ) と呼ばれる値により、機器の種別を知ることができる。ゲートウェイは、Discovery にて検出した ECHONET 機器が持つ EOJ の値に応じて、Device Description/Service Description と呼ばれる UPnP のデバイス/サービス内容を表す情報を提供する。
- (3) **Control** ゲートウェイは、UPnP コントローラから送られてくる UPnP 制御要求メッセージを、ECHONET 制御要求メッセージへと変換し、制御対象となる ECHONET 機器へと送信する。同様に、ECHONET 機器から受け取った ECHONET 制御応答メッセージを、UPnP 制御応答メッセージへと変換し、UPnP コントローラへ返送する(図 2)。
- (4) **Eventing** ゲートウェイは、ECHONET 機器からのマルチキャストによる状態変化通知メッセージを検出した場合、UPnP コントローラから事前に受け付けていた通知検出依頼と内容が合致しているか調べる。合致しているならば、その ECHONET メッセージを UPnP 通知応答メッセージへと変換し、UPnP コントローラへ送



信する。

Description での機器情報や Control でのメッセージ変換方法は、機器種別ごとに定義される。これらは ECHONET-UPnP ゲートウェイ仕様として、エコーネットコンソーシアムにより標準化が進められている。

以上のようなマッピング方法を用いることで ECHONET-UPnP ゲートウェイは、UPnP による AV 機器や白物家電の統合的な制御を可能にする。なおこの章では、UPnP コントローラから ECHONET 機器を UPnP により制御する機構について示したが、逆の ECHONET コントローラから UPnP 機器を ECHONET により制御する機構についても、ゲートウェイの機能として標準化が進められている。

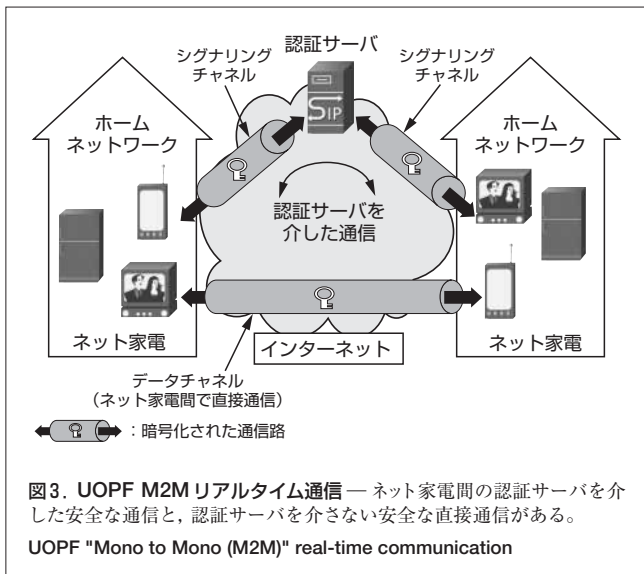
### 3 UOPF

“誰でも、簡単に、安全に” ネット家電をインターネットに接続できるようにするため、国内の ISP (Internet Service Provider) や家電メーカーを中心として UOPF が 2004 年に発足した。東芝も発足時から参加し、積極的に仕様化に取り組んでいる。この章では、ネット家電間の安全な通信路を確立するための“M2M (Mono to Mono) リアルタイム通信”と、確立された安全な通信路でネット家電遠隔制御を実現する“UOPF リモートコントロール”について説明する。

#### 3.1 UOPF M2M リアルタイム通信

UOPF M2M リアルタイム通信とは、SIP (Session Initiation Protocol) と呼ばれる本来 IP (Internet Protocol) 電話などの呼制御を目的としたプロトコルをベースに、セキュリティ確保などの機能を拡張した通信方法である。次の 2 種類の通信方法を規定している(図 3)。

- (1) 認証サーバを介した安全な通信 認証サーバがネット家電間の通信メッセージを転送する方法
- (2) ネット家電間の安全な直接通信 認証サーバを経由せずにネット家電間で直接通信メッセージをやり取り



する方法

### 3.1.1 認証サーバを介した安全な通信

複数のネット家電と安全な通信を行う場合、通信相手となるネット家電ごとにユーザー ID (IDentification) やパスワードなどのセキュリティ設定が必要となる。このためセキュリティ設定が煩雑になってしまう。この問題を解決するために UOPF M2Mリアルタイム通信では、ネット家電から見て信用できる認証サーバがネット家電間の通信メッセージを転送する仕組みを導入している。

ネット家電は SIP ユーザーエージェント (SIP 端末) としての機能を持っている。最初に、ネット家電は SIP プロキシサーバの機能を持つ認証サーバと通信して認証を受けた後、暗号鍵を交換する。これにより、ネット家電 - 認証サーバ間に暗号化された安全な通信チャンネル (シグナリングチャンネル) が確立される。このプロセスは SIP 端末を登録するための SIP 標準仕様である REGISTER リクエストを拡張した方式を利用している。このシグナリングチャンネル上で、認証サーバが認証済みネット家電間のメッセージを転送することで、ネット家電間の安全な通信が可能となる。この方式では、ネット家電は直接の通信相手となる認証サーバに対するセキュリティ設定だけを行えばよいため、ネット家電のセキュリティ設定が簡単化される。

### 3.1.2 ネット家電間の安全な直接通信

3.1.1 で確立した安全なシグナリングチャンネルを利用すればネット家電間における通信の安全性は確保される。しかし、認証サーバがすべての通信メッセージを転送するため認証サーバの負荷が高くなり、通信のリアルタイム性を損ねてしまう問題がある。そこでネット家電は、通信パラメータを交換するための SIP 標準仕様である INVITE リクエストを利用して、安全なシグナリングチャンネル上で相手ネット家電と暗号鍵を交換す

る。ネット家電はこの鍵を用いて、認証サーバを介さず直接ネット家電間に安全な通信チャンネル (データチャンネル) を確立し通信を行う。これにより認証サーバに負荷をかけず、ネット家電間で安全な直接通信が可能となる。

## 3.2 UOPF リモートコントロール

UOPF リモートコントロールは、宅外からのネット家電の操作及び監視や、ネット家電から宅外への状態通知を実現するための、M2Mリアルタイム通信を利用した遠隔制御方式を規定するものである。

### 3.2.1 制御コマンド転送フレームワークの提供

遠隔端末とネット家電間の制御コマンド転送には、M2Mリアルタイム通信の仕組みで認証し暗号化がなされたシグナリングチャンネル、あるいはデータチャンネルが利用される。

シグナリングチャンネルを利用する場合、ネット家電の操作や監視は、IM (Instant Messaging) のための SIP 標準仕様である MESSAGE リクエストを利用して実現する。ネット家電からの通知には、イベント通知のための SIP 標準仕様である SUBSCRIBE/NOTIFY リクエストが利用される。データチャンネルを利用する場合、使用するプロトコルは、基本的には HTTP (HyperText Transfer Protocol) を想定しているが、L2TP (Layer2 Tunneling Protocol) などのほかのプロトコルも、データチャンネル確立時のネゴシエーションによって選択可能な仕組みとなっている。

UOPF リモートコントロールは、以上のような制御コマンド転送のためのフレームワークについては規定しているが、制御コマンドのフォーマット自体については規定していない。これは、UOPF リモートコントロールの基本的な設計ポリシーとして、UPnP などの既存のコマンド体系を、そのまま利用することを想定しているためである。

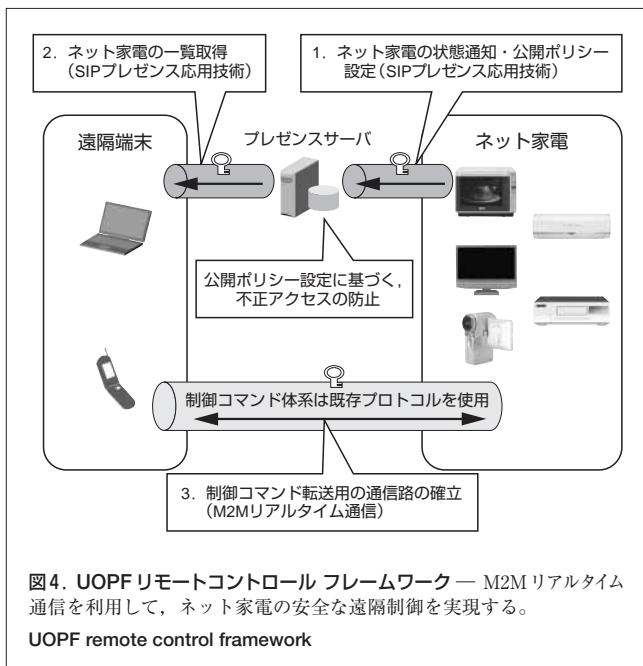
### 3.2.2 SIP プレゼンスを利用したネット家電情報の収集

UOPF リモートコントロールは、SIP のプレゼンスサービスを応用した、ネット家電情報を収集する手法についても規定している。

IP 電話システムにおける一般的なプレゼンスサービスは、不特定多数の通信相手に対し、みずからの通話可否状態や場所を公開するためのものである。他方、遠隔制御や監視のためのネット家電情報は、所有者だけが利用するものであり、他人に公開するものではない。このため、UOPF は、ネット家電情報の公開ポリシーをプレゼンスサーバ (プレゼンス情報を管理及び提供するサーバ) に設定する手法を規定している。これにより、ネット家電への他人の不正アクセスを防止したり、家族だけがアクセスできるように柔軟に設定することが可能となる。

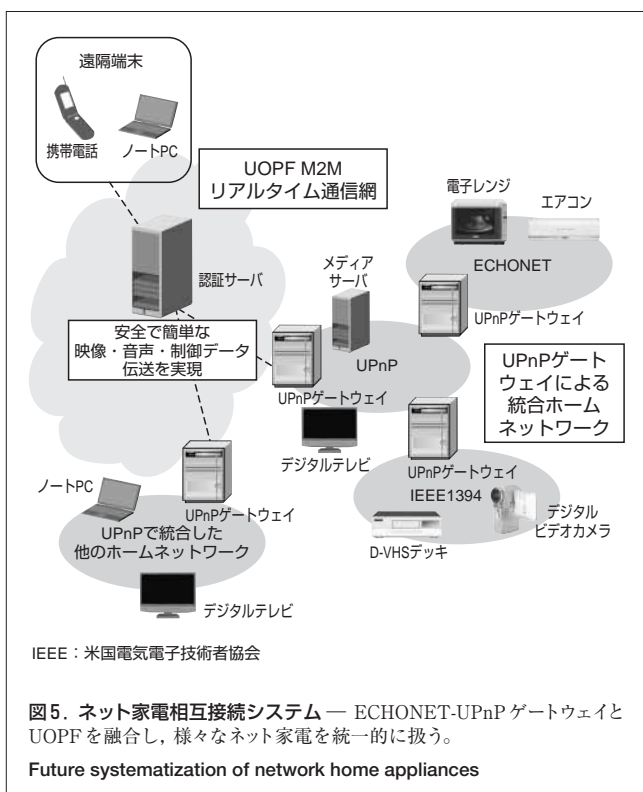
UOPF リモートコントロールは、遠隔端末がネット家電を発見し、制御コマンドを伝送するための安全な通信路を確保するまでの汎用的な手法を提供するものであると言える (図4)。





#### 4 今後の展望

2章で述べたECHONET-UPnPと3章で述べたUOPFは、相互補完的な技術であり、将来的には双方を組み合わせることによって、インターネットを介した統合的なネット家電相互接続システムが実現できる(図5)。



ECHONET-UPnPゲートウェイ技術を応用することによって、ECHONET以外のプロトコルに対応したネット家電も、UPnPで統一的に扱うことが可能となる。一方UOPFリモートコントロール技術が、このUPnPで統合されたホームネットワークと携帯端末、あるいはホームネットワークどうしを、インターネットを介して安全に接続する。更に、UOPFの基盤技術であるM2Mリアルタイム通信は、制御コマンドだけでなく、音声・映像ストリーム伝送の枠組みをも提供する。

したがって、このネット家電相互接続システムは、音声・映像・テキストベースであらゆるネット家電と通信可能な枠組みを提供するものであり、単なるテレビ電話やリモートコントロールにとどまらない、多様なサービスを実現する基盤になりうるものと言える。

#### 5 あとがき

ここで述べたECHONET-UPnPゲートウェイ、UOPF M2Mリアルタイム通信、及びUOPFリモートコントロールの技術を利用することにより、家庭の内側(ホームネットワーク)と外側(インターネット)の両方のネットワークで、簡単に安全にネット家電間の通信ができる基盤が整いつつある。そして、この基盤の上に高度なネット家電向けアプリケーションの構築が可能となり、ユーザーに多様なサービスを提供できるようになる。今後とも、これらの技術の標準化活動などを通して、更なるネット家電の普及を目指していく。



神田 充 KANDA Mitsuru

研究開発センター 通信プラットホームラボラトリー研究主務。  
ネットワークプロトコルの研究・開発に従事。  
Communication Platform Lab.



寺島 芳樹 TERASHIMA Yoshiaki

研究開発センター 通信プラットホームラボラトリー。  
ネットワーク家電の研究・開発に従事。  
Communication Platform Lab.



安次富 大介 AJITOMI Daisuke

研究開発センター 通信プラットホームラボラトリー。  
ネットワーク家電の研究・開発に従事。  
Communication Platform Lab.