TTC技術レポート
Technical Report

TR-1053
サービスプラットフォームにおける
カスタマサポート機能

Customer support functions

for home network service platform

第1.1版

2016年2月23日制定

一般社団法人
情報通信技術委員会
THE TELECOMMUNICATION TECHNOLOGY COMMITEE

TTC Telecommunication Technology Committee

本書は、一般社団法人情報通信技術委員会が著作権を保有しています。
内容の一部又は全部を一般社団法人情報通信技術委員会の許諾を得ることなく複製、転載、改変、転用及びネットワーク上での送信、配布を行うことを禁止します。

目　次

＜参考＞

１．　国際勧告等との関連

本技術レポートに関する国際勧告は本文中に記載している。

２．改版の履歴

版数	制定日	改版内容
第1.0版	2014年3月20日	制定
第1.1版	2016年2月23日	改訂 誤記訂正（障害、故障の誤用）

３．参照文章

主に、本文内に記載されたドキュメントを参照した。

４．技術レポート作成部門

第１．０版　：　次世代ホームネットワークシステム専門委員会　（SWG3603）

第１．１版　：　次世代ホームネットワークシステム専門委員会　（SWG3603）

５．本技術レポート「サービスプラットフォームにおけるカスタマサポート機能」の制作体制

本技術レポートは、新世代ネットワーク推進フォーラムIPネットワークWG　レジデンシャルICT SWG(リーダー: 丹康雄[JAIST/NICT])において原案を作成し、その後TTC次世代ホームネットワークシステム専門委員会(委員長: 山崎毅文[NTT])での審議を経てTTC技術レポートとしてとして公開するものである。

レジデンシャルICT SWGにおける検討においては、戦略ビジョンタスクフォース(主幹:松倉隆一[富士通])のもとにアドホックグループを形成して作業にあたった。

第1章　はじめに

本技術レポートでは、ホームネットワーク（HN）に接続されたデバイスを利用するサービスを実行する際に発生する各種の障害（failure）に対して、遠隔からの原因分析、障害復旧作業において必要となるモニタリングや設定変更、障害診断機能などの、サービスプラットフォーム（PF）に備えるべきカスタマサポート機能について述べる。

1.1　背景

ブロードバンドネットワークの普及に伴い、家庭内のデバイスが相互に接続されHNを構成するようになった。HNでは、白物家電、黒物家電（AV家電）、セットトップボックス（STB）/ホームゲートウェイ（HGW）、銀物家電（PC、スマートフォン、タブレット）、ゲーム機など、設置や保守の考え方、ネットワークへの接続方法、求められる品質の異なるデバイスが混在している。こうした複雑なネットワークを構成するHNでは、デバイスが接続できない、映像が映らないなどの障害が発生したときに、同時に動作している複数のシステムのどこに問題があるかを特定することが困難である。また、HNでは設置や動作環境の維持はエンドユーザが担うことが多く、専門家である管理者は現場には不在であり、遠隔からの管理が前提になっている。今後、HNサービスが進化するにつれて、障害からの復旧プロセスを遠隔から実現する仕組みは重要になる。

TTC技術レポート「ホームネットワークサービスを実現するサービスプラットフォーム」（TR-1046）では、HNに接続されるデバイスを利用してサービスを構築するためのサービスプラットフォームについて述べている。上記で述べたような障害への対応プロセスを、TTC TR-1046に記載されるサービスプラットフォームに予め備えることによって、デバイスとサービス開発、設置工事と保守運用までを含めてトータルに扱うことができる。本技術レポートでは、HNサービスにおける障害事例を元に原因を分析し、分析結果に基づいて障害から復旧するための技術について検討したうえで、遠隔から障害原因の特定と障害からの復旧プロセスを支援するシステムについて説明し、サービスプラットフォームでの機能配置について述べる。

1.2　HN サービス向けプラットフォーム

HN サービスは、HN に接続されるデバイスを制御することで実現される。HN に接続可能なデバイスは年々増えている。黒物家電は国内で出荷されるデバイスの多くが DLNA をサポートし、白物家電は ECHONET Lite への対応が進みつつある。また、アプリケーションをインターネットやクラウドで実行することが珍しくなくなっているため、本技術レポートでもクラウドでのサービス提供を前提に検討を行う。HN サービスプラットフォームのアーキテクチャについては、TTC TR-1046 に記載されており、本技術レポートでもこの TTC TR-1046 に基づくものとする。TTC TR-1046 に記載されるアーキテクチャを図 1-1 に示す。

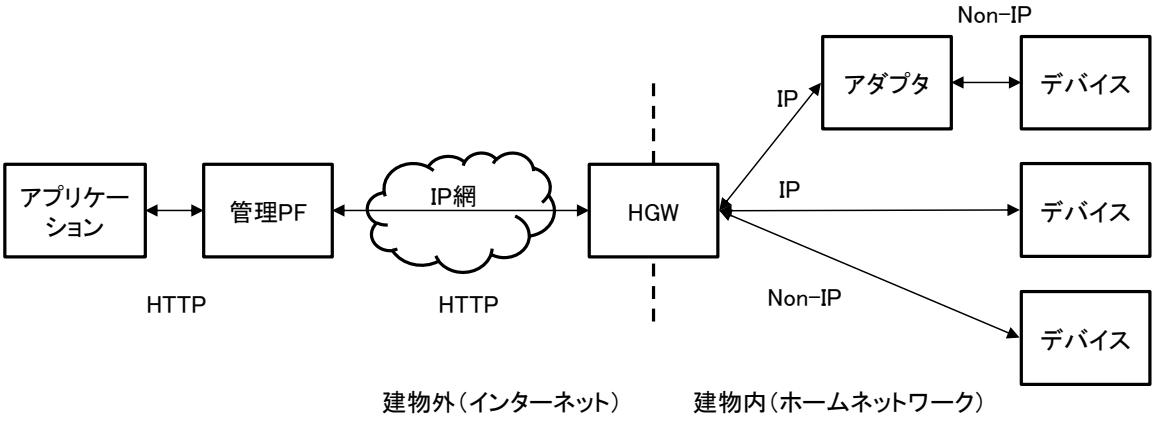

図 1-1 サービスプラットフォームのアーキテクチャ(TTC TR-1046)

HN に接続されるデバイスとしては、ECHONET Lite に対応したデバイスを想定している。ECHONET Lite は、ECHONET コンソーシアムが住宅に設置される 80 種類以上のデバイスについて、そのデバイスが保持する情報やリモートで操作可能な制御項目（プロパティ）を論理的なモデル（機器オブジェクト）として規定している。TTC TR-1046 で規定するサービス PF では、この論理的なオブジェクトを HGW を経由して管理 PF 上に仮想的なデバイスとして表現し、この仮想的なデバイスのアプリケーションから参照、操作することでデバイスを制御するようにしている。ECHONET Lite と同様な規格は、欧州の KNX や米国で普及する ZigBee Smart Energy Profile(SEP) 2.0 等があり、国内だけでなく、海外でもこのアーキテクチャは適用可能と考えている。また、デバイスが ECHONET Lite に対応していない場合でも、アダプタを接続することで ECHONET Lite に対応することも可能である。また、アダプタ機能を HGW に備えることも可能であり、デバイスの接続方法は柔軟になっている。ホームゲートウェイ（HGW）は HN 内の接続を終端して、インターネットに接続される。管理 PF はインターネット経由で HGW と接続し、住宅内のデバイスの情報をモニタしたり制御することが可能である。具体的なサービスは管理 PF が用意する API を利用して開発される。

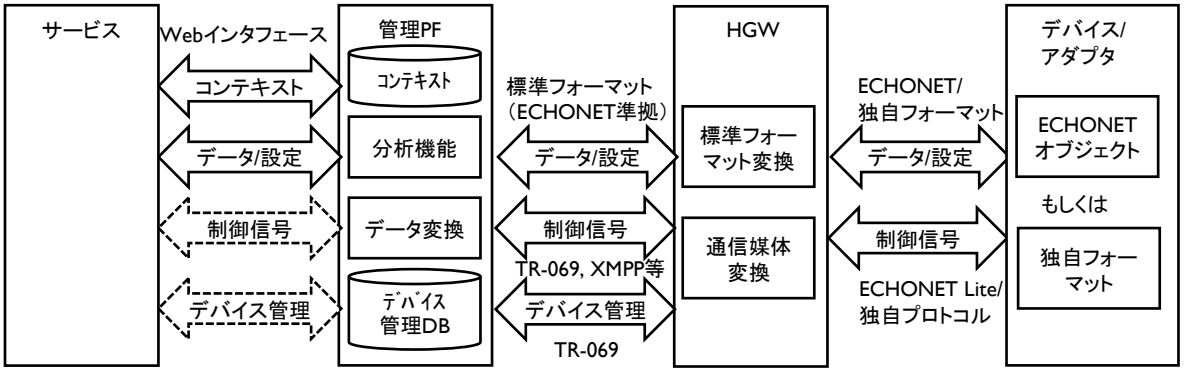

図 1-2 機能アーキテクチャ(TTC TR-1046)

図 1-2 には機能アーキテクチャを示した。それぞれのノードの機能は以下の通りになっている。

・デバイス

アダプタを利用して HGW に接続するケースでは、アダプタのインタフェースをデバイスのインタフェースとして表現した。デバイスは、通信手順（制御信号）とデータフォーマットとを独立させて、方式として共通化できるようにする。通信手順としては、設定変更（SetDeviceProperty）、状態参照（GetDeviceProperty）、状態通知（Inform）からなり、データフォーマットはデバイスの属性名と属性値の組で表現されるものを基本とする。

・ホームゲートウェイ（HGW）

ホームゲートウェイ（HGW）は、HN と WAN との通信の中継を行い、通信の物理媒体とプロトコルの変換を行う。

上位レイヤにおけるプロトコル変換としては、ECHONET Lite で定義されるデータ通信手順（GET/SET/INFORM）とデータフォーマットの変換を行う。WAN 側の通信はデータフォーマットを XML 化して、HTTP で通信することが考えられる。このプロトコルの候補の一つとして、BBF TR-069 が挙げられる。ECHONET Lite での通信手順と BBF TR-069 の GetParameterValue / SetParameterValue 等との対応を実現し、データフォーマットを BBF TR-181 に合わせて XML 化することで、HGW で透過的に中継することが可能である。

・管理PF

管理 PF は、HN に接続されるデバイスとアプリケーションとの橋渡しの役割を果たす。HN に接続されるデバイスは、HGW を経由して仮想デバイスと表現される。仮想デバイスは、ECHONET の機能オ

ブジェクトを XML で表現したデータ形式であり、実際に接続されるデバイスやネットワークは別途端末管理 DB に記録される。一方、アプリケーションに対しては、アプリケーションの管理・連携機能を持つ。アプリケーション管理・連携機能は、アプリケーションを実現するための基本機能として、UI、分析機能、データ変換がある。ほかに重要な機能として、複数のサービスが連携するための機能が存在する。TTC TR-1046に記載されるユースケースでは、行動把握、診断結果、スケジュール、デバイス状態、故障（fault）、各種イベントがアプリケーション間を結ぶ情報として、互いに通知、もしくは参照可能である。

・アプリケーション

アプリケーションは、管理 PF で提供する API を利用して動作する。サービス提供者は独自のサーバを運用するケースや、管理 PF を運営する事業者サーバで動かすケースなどが考えられる。

TTC TR-1046 ではアプリケーションをサービスと記載している。サービスはシステム全体を示す意味があるため、本技術レポートでは、プラットフォーム上で動作するアプリケーションと限定する表現に変更する。

第2章　ユースケース

2.1　障害事例

2章では、HNサービス向けのプラットフォームの課題とその解決に求められる機能について検討する。HNの構成が複雑化し、接続されるデバイスが増えるにつれて、様々な障害、不具合が発生しうる。ここでは、実際の障害事例に基づいて、原因分析を行うものとする。

事例はHNの不具合に限定されない。HNサービスにおける障害は、接続されるデバイス、ネットワーク、アプリケーションと、それらの組み合わせやユーザの操作ミスなどにも原因があると考えられ、多くの観点から検討する必要がある。また、現時点では利用者自身が対応しなくてはならない事例でも、遠隔サポート機能により問題の切り分けや課題解決を期待できる可能性がある。そこで、ユースケースとして範囲を限定することなく障害事例を求めたところ、以下の表2-1の事例が紹介された。

表 2-1. 障害事例

	課題	概要
1	サービス間の干渉	ガスメータの検針システム（ノーリンギングサービス）を利用中のお客様がインターネット利用のためにADSL回線（電話重畳型）の申し込みをしたところ、ガスメータの検針システムとの干渉のため利用できなかった。
2	通信帯域の占有	特定のデバイス（レコーダ系機器など）に通信帯域を一時占有するものがある。またゲーム機の通信機能（ファームアップ、ファイルダウンロード、通信対戦）で通信帯域を圧迫する場合がある。デバイスの通信特性はユーザに認識されていない。
3	経年劣化による誤動作	ガス漏れ検知システム（買取）の誤作動で大きな警報がなったが、ガス漏れはなかった。家庭では耐用年数を過ぎても使い続ける場合があり、リコール対象デバイスも放置される場合あり。
4	既設無線デバイスとの干渉	新規購入したPCの無線LANがつながらないという顧客クレーム。既存PCの無線LANは動作しているので、新PCのデバイス不良が疑われたが、現地調査でワイヤレスAVデバイス（5.1chサラウンドスピーカー）との干渉が原因と判明した。
5	他端末の影響	HN内のNAS（HDDレコーダー機能付き）上のデータを同ネットワーク内PCの専用ソフトで再生しようとしたが、通信が遮断され再生できない。PC上の別ソフトウェアの不具合により、PCが受信したデータが欠損することが原因の模様。
6	サイレント故障 （一部機能停止）	光TV、HDDレコーダーの環境において、2週連続で特定の放送の録画が音声だけになっていた。その放送の直前の番組は正しく録画されている。また他の放送も正しく録画されている。その後何も対処していないが、3週目以降は正しく録画出来ている。デバイス単体の故障と通信の故障の切り分けが必要。
7	サイレント故障 （サービス停止）	家族から固定電話がつながらないと連絡をもらい不具合に気づいた。パソコンからインターネット利用できていたので、いつから電話が止まっていたか判らない。サポートに連絡して、指示通りに終端装置を再起動したら電話が使えるようになった。常時動いていると思い込んでいるサービスであり、サービス停止に気づかない。
8	誤った使い方による障害	介護事業者の見守りサービス関連。介護者自身が節電のために、見守りシステムの電源をオフにしたため、有効な見守りができなくなった。 介護者自身が見守りシステムのペンダント式端末をトイレに置き忘れた。一定期間、移動や振動を検知しない場合は、看護ステーションに連絡が入るシステムになっており、緊急対応が発生した。
9	起動順序による障害	終端装置と通信機能付きデバイスの問題。停電の際に、供給復帰が一斉であっても、各々のデバイスは、起動から通信機能復帰まで特定のプロセスで立ち上がるため、起動の順番、タイミングによってはアドレスがうまく取得できないケースがある。
10	設定ミスによる障害	インストール工事時の設定ミスにより障害が発生。

2.2 原因分類

前項の表2-1の事例について、その原因を分析し、どの区間で何が起きているかについて検討を行った。その結果をまとめたのが以下の表2-2である。障害事例の()内の数字は、表2-1の障害事例の項目番号を示す。

表 2-2. 障害事例における原因分類

ネットワーク	レイヤ	障害事例		障害原因
		インストール段階	運用段階	
HN	利用者		誤った使い方による障害(8)	ユーザの勘違い等による操作ミスによる障害。以下のレイヤでは障害と認識されない。
	サービス干渉	他端末の影響(5) 起動順序による障害(9)	他端末の影響(5) サイレント故障(6)	端末、サービス、ネットワーク単体では問題がなく、組み合わせによって生じるもの。
	端末	設定ミス(10)	経年変化による誤作動(3) サイレント故障(7)	端末のハードウェア、ソフトウェアに起因する障害。
	ネットワーク		通信帯域の占有(2) 既設の無線デバイスとの干渉(4)	ネットワークの帯域不足による障害。他のトラフィックが多い、無線チャネルの干渉等による通信品質低下による障害。
WAN	サービス または ネットワーク	サービス間の干渉(1)	通信帯域の占有(2)	ネットワーク特性（帯域、回線種別）とサービス要件のミスマッチ

表2-2では、原因がネットワークのHN/WANのどちらに起因するかを分類したうえで、HNについてはネットワーク、端末、サービス干渉、利用者の4つのレイヤに分類することとした。以下で詳細を述べるが、ここで端末とは、図1-1に示すデバイスのほかに、ネットワーク機器も含んでいる。サービスプラットフォームでは、アプリケーションレイヤでのアーキテクチャについて主に述べているが、HNサービスのカスタマサポートという観点ではネットワークレイヤの機能についても触れる必要がある。そのため、以下ではサービスプラットフォームにおけるデバイスとネットワーク機器を「端末」と呼ぶことにする。

(1)HNとWANとの切り分け

不具合解消のために原因区間の切分けから着手される。具体的には、図1-1のHNのアーキテクチャを前提としたとき、はじめに建物内の問題（HN区間）と建物外の問題（WAN区間）の切り分けが重要になる。

WANについては通信事業者やサービス事業者の責任区間であり設備やサービスについて管理が行われている。他方、HN区間を統合して管理をする事業主体が不在であり、管理PFがその役割を担うことが期待される。

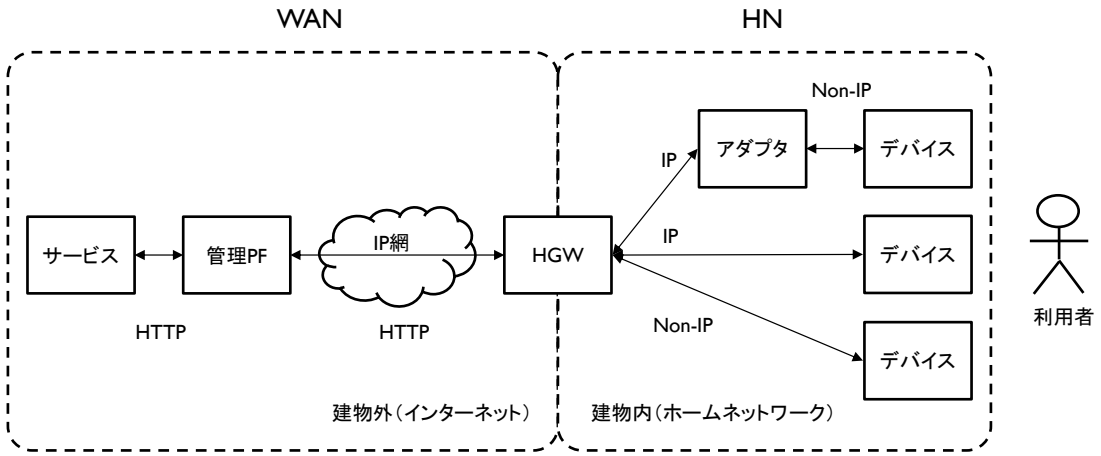

図 2-1 WANとHNの区分

(2)レイヤの考え方（HN/WAN）

次に「レイヤ」による区分を設けて整理をした。

具体的には「ネットワーク」、「端末」、「サービス干渉」、「利用者」の4つの区分で整理を試みた。

「ネットワーク」：輻輳や通信帯域の不足、無線チャネルの干渉などの不具合

「端末」：　端末単体の不具合とし、ハードウェアやソフトウェアに起因する障害

「サービス干渉」：端末、ネットワークともに単体では問題がないが、同時に利用をしようとすると問題が発生する不具合

「利用者」：　利用者自身の操作ミスやサービスの理解不足によるもので、上記の３つの区分では不具合とは認識されない

なお、WANにおいてもレイヤ毎に障害事例と原因が考えられるが、今回はHNにおける検討に集中するためにHNに直接関係する原因についてのみ記載した。WANにおける障害と原因分析については別の機会に実施する。

第3章　要素技術

3.1　概要

本節では、2.2で分析した個々の原因に対して、それぞれ解決する既存技術、将来必要となる技術について説明する。ここで説明する機能は、カスタマサポート機能と障害回避支援機能の2種類からなるため、はじめにその概要を説明する。

(1)カスタマサポート機能

HNを利用するカスタマがインストール段階において、デバイスの全体構成とその設定について円滑に行えるように環境の整備が必要となる。仮にネットワーク上で競合するハード、アプリ、サービスの事前チェックなどを行う機能が端末へ搭載されていると該当する問題点をカスタマに通知することができる。一方、運用段階においては、デバイスの設定情報やネットワーク接続性さらには、利用状況の確認を行ったり、ネットワークのトラフィック情報や負荷に対する耐用の確認を通知する機能が端末に搭載されていると安心してその端末を利用することができる。

(2)障害回避支援機能

HNを設定する際、端末のガイドラインに基づきその対応を行ってもカスタマの操作ミスで設定ミスによる障害が発生する可能性もある。このような設定ミスによる障害が起こった場合、自動的にデバイスの設定を行う機能（デバイスの自動発見・設定・起動順序制御）が端末またはアダプタに搭載されていると障害回避支援を行うことができる。また、運用段階においては、トラフィック制御（メディア種別、アプリ種別等）による帯域保証機能が、端末またはアダプタと連携するHGWとの間で対応されることが望ましい。

上記を踏まえ、表3-1に各レイヤに望まれる機能を整理した。以下の節では、この詳細について説明するが、システムを構成する最小単位としての端末、ネットワーク（HN/WAN）、アプリケーション関連の順序で説明する。

表3-1 各レイヤに望まれる機能

ネットワーク	レイヤ	項目	望まれる機能
HN	ユーザ	ユーザ行動チェック	ユーザ誤操作検出：操作履歴等から「いつもと違う」操作、状態を検出する
	サービス干渉	リソース組み合わせチェック	サービス干渉検出：端末、端末上で動作するソフトウェア、通信プロトコル間の干渉の恐れのある組み合わせを判断
	端末	白物（家電）	基本機器情報取得：型名や設置時期を取得して経年劣化による故障かを判断する（ECHONET/DLNA等） 端末接続確認：ネットワーク到達可能であることの確認（ICMP等） 端末動作情報取得：デバイスステータス、エラー情報、統計情報を取得して障害要因を特定（ECHONET/DLNA等） トータル情報管理：端末の契約情報を取得（資産管理等） 端末自動設定：端末の設定情報を外部から取得し、設定する機能
		黒物（AV機器）	
		銀物（PC/スマートフォン）	
		ネットワーク機器	
	ネットワーク	負荷試験ツール	基本計測機能：基本的なMIBの統計情報（TTC HTIP、SNMP）の取得 低位レイヤ負荷試験：ping flooding、netperfによるネットワーク負荷ツールを利用した試験 アプリケーションレイヤ負荷試験：負荷発生装置による試験
WAN	サービス/ネットワーク	サービスチェック	ネットワークレイヤ競合チェック：SNMP、OAM等を利用して取得した情報による競合関係のチェック アプリケーションレイヤ競合チェック：BBF TR-069、UPnP DM等を利用して取得した情報による競合チェック
		評価ツール	接続状態：トラフィック情報収集 帯域制御： QoS制御

3.2 端末での課題を解決する機能

HNサービスを構成する要素として、最も基本的な端末から説明する。端末の課題を解決するには、端末が障害解決や自動設定に必要なインタフェースを用意することが必要である。障害解決に必要なインタフェースとしては、内部情報を取得するためのものがある。内部情報としては、端末がHNに接続されて最小限動作するために必要な設定情報から、資産管理や情報管理のために所有者や契約情報まで様々なものがあり、3.2.1～3.2.4にて各視点での情報取得について説明する。また、3.2.5では設定可能な情報について、端末の外部から設定するための仕組みとして自動設定機能について説明する。端末と通信するのはHGWである。HGWはさらにWAN側に中継してインターネットサーバやクラウドで端末の管理を実現する。

3.2.1 端末基本情報取得

端末は、①白物家電　②黒物家電　③銀物家電　④ネットワーク機器である。ただし、ECHONETにおいて、機器オブジェクトとして定義されているデバイスは白物家電相当として扱う。また、テレビのように①白物家電と②黒物家電の両方の定義がある場合には、白物家電として扱うか、黒物家電として扱うかによって機能が異なると解釈する。①～④に属しないデバイスについては、ECHONETの枠組みで接続することとして白物家電とみなすことにする。

端末からの情報取得を行うことで経年劣化による故障や故障時期の判別、リコール対象製品がどこで利用されているか、また、ネットワーク機器では、他との連携において性能が充足しているかどうかの判断を行

える。これらの情報取得を行うには、端末のメーカ名と製品情報（型名・製造年月日・ハードウェアやソフトウェアに関する情報（CPU、メモリ容量、OS））と設置情報（設置業者・設置年月日・設置場所・設置治具（給湯器の配管・PVの架台情報等））の情報がある。端末の情報取得を管理する手段としては、HGWと端末間（アダプタ経由の接続を含む）にて標準プロトコルを利用してHGWにデータを収集し、クラウドで収集した端末情報を管理することが考えられる。標準プロトコルとしては、ECHONET Lite、DLNA、UPnP等が候補である。ECHONET Liteではデバイスのエラーコードを取得するインタフェースが規定されているため、こうした情報を利用してシステム管理者は、クラウドに収集された情報を保守用インタフェースで参照し、障害解決を行うことができる。

3.2.2 端末接続確認

HNにおける端末の接続確認は、HGWから端末にメッセージを送信し、応答を確認することで実現できる。ただし、途中経路のネットワーク機器に問題がある場合には、HNのトポロジー情報を参照するなどして、部分ごとに調査していく必要がある。

HGWと端末（アダプタ経由の接続を含む）との間は、様々な通信インタフェース（Wi-Fi、PLC、ZigBeeなど）が利用され、HUBやアクセスポイント、ゲートウェイで接続される。センサなどの非IP端末を無線通信で接続する場合には、端末のハードウェアリソースの制約のために、定期的にHGWから接続確認（ポーリング）を行う方法により確認状況を管理する必要がある。また、HGWと端末の間は、ネットワーク機器を経由して接続されるケースもあるため、単にHGWと端末間の接続を確認するだけでなく、経路上の各区間で問題がないことを確認する必要がある。そのため、HNのトポロジーを取得するTTC HTIP（ITU-T G.9973）やIETF ICMP、IETF SNMP、LLDP、UPnP等のサポートが期待される。

3.2.3 端末動作情報取得

端末の動作情報は、3.2.1で述べた基本情報以外に障害解析に必要と考えられる情報を含んでいる。取得される具体的な情報としては、利用頻度（連続使用期間、使われなかった期間）、端末の再起動や障害等の各種イベントのログ、基本情報としては扱われない端末の内部状態など、端末が安定して動作しているかを把握するために有用と考えられる情報があげられる。サービス停止時の障害解析に使用したり、障害が疑われる端末と連動している端末を接続し、その影響を調査する場合に利用する。

なお、管理項目として、デバイスの操作記録・デバイスの内部状態の時系列データ・デバイスの障害解析用ログ（ログの詳細レベルの変更可能）が考えられる。管理方法は、ECHONET Lite、DLNA等の通信プロトコルを利用して、デバイス操作の取得や・障害解析用ログ情報を記録し、収集する手段が考えられる。

3.2.4 トータル情報管理

トータル情報管理は、端末の資産管理という観点から、端末がHNに接続されてサービスで使用され、サービスの利用終了時に端末がHNから取り外されるまでの間に管理される全ての情報を扱う。例えば、端末をメーカの定める耐用年数を超えて使用した場合に、使用開始時期が不明なままでは耐用年数を超過していることを判断することができない。そのため、トータル情報管理では、端末の設置年月日、所有者や契約形態のような情報も含めて管理する。トータル情報管理は、家電や住宅設備のような組込み機器より、PCやスマートフォンのような銀物家電が対象であることが多い。図3-1では資産管理システムによって、端末に関わる情報を管理する場合の構成を記載した。端末であるPCやスマートフォンに対しては、OSに資産管理ソフトをインストールし、管理サーバからの要求に応じて、端末情報を管理サーバに収集する。

管理項目（インベントリ情報）は、本体ハード（PC/スマートフォン等：CPU型番、メモリ容量、HD容量、OS種別・バージョン、IPアドレス）や運用情報（所有・契約形態、設置場所、利用者/管理者、取得年月日）

ソフト（インストールされているソフトウェア、ライセンス内容、利用頻度）、セキュリティ（ウィルス対策ソフト/ブラウザ等の設定、証明書等の管理）が考えられる。

図3-1. 資産管理システム

端末で取得される情報について、3.2.1～3.2.4で4つの視点から述べた。しかし、この4つの観点で取得される情報の、それぞれの範囲に関して明確な定義が存在するわけではない。したがって、具体的に取得されるべき端末の情報については、ユースケースの中で明確にされることになる。

3.2.5 端末自動設定

HNにおける端末の設定ミスは、HNと接続できない、動作しないという明確な障害として露見する場合もあるが、要因として潜在して特定が難しいケースも多い。専門家でないユーザが端末を設置する場合や、専門家が設置する場合でも大量に設置するときには、設定ミスは発生しやすくなる。したがって、端末の設定情報を集中的に管理して、導入時に自動的に行う機能は設定ミスの削減に有効な手段である。また、自動設定機能は端末の導入時だけでなく、HNの構成を変更するときや端末のソフトウェアをアップデートするときにも有効である。

図3-2に自動設定における基本的なシステム構成を示す。端末には設定エージェントが存在し、このエージェントがHGWもしくはインターネット上のサーバに問い合わせを行い、設定情報を取得する。これを実現する通信規格としては、端末をネットワーク機器として扱うか、家電として扱うかによって異なるため、以下では、それぞれについて説明する。

図3-2. 自動設定システム

(1)ネットワーク機器としての自動設定

IPv4通信において、IPアドレス、DNSサーバアドレスといったIP通信に必要なパラメータを端末に設定するためのプロトコルとして、IETF RFC2131で規定されるDHCP（Dynamic Host Configuration Protocol）が存在する。パラメータの払い出しを行うDHCPサーバ機能は、HNでは通常、ブロードバンドルータやHGWといったWANとの接続を行うネットワーク機器が提供する。

IPv6通信において、IPv6アドレスを端末に設定するためのプロトコルとして、IETF RFC3315で規定されるDHCPv6（Dynamic Host Configuration Protocol for IPv6）と、IETF RFC4861で規定されるRA（Router Advertisement）が存在する。また、DNSサーバアドレスといったIP通信に必要なパラメータを端末に設定するためのプロトコルとしてDHCPv6が用いられる。パラメータの払い出しを行うDHCPv6サーバ機能やRA送信機能は、HNでは通常、ブロードバンドルータやHGWといったWANとの接続を行うネットワーク機器が提供する。

(2) 家電としての自動設定

アプリケーションレベルの通信に必要な自動設定のための機能は、アプリケーションプロトコルが提供する。例えば、ECHONET Liteでは、ECHONET Lite対応端末を発見するための通信手順や、ECHONET Lite対応端末が管理するECHONET Liteオブジェクトに何があるかの情報を取得するための通信手順が用意されている。別の例として、UPnPでは、UPnP対応端末を発見するための通信手順や、UPnP対応端末が実装する機能に何があるかの情報を取得するための通信手順が用意されている。

3.3 HNでの課題を解決する機能

本節では、HNサービスを構成する要素として、HNに接続される端末のネットワークについて説明する。HN課題の解決としては、ネットワーク機器の設定に関する問題について3.2節で述べたので、HN内のトラフィックに起因する課題解決方法について3.3.1～3.3.3で説明する。

3.3.1 基本計測機能

HNにおける基本計測機能として、構成情報取得機能と統計情報取得機能の2つが挙げられる。構成情報取得機能は、トラブルシューティングに必要な、ネットワークを構成する端末間の接続関係や、各端末の構成情報を取得するために利用可能である。統計情報取得機能は、ネットワークを構成する端末の動作状態を把握するために利用可能である。以下に、各々の内容について説明する。

(1) 構成情報取得機能

構成情報取得機能は、カスタマサポート対象となるシステムを構成する、ネットワーク機器を含む各端末の構成に関する情報を取得する機能と定義する。構成情報の例として、以下のものが挙げられる。（図3-3）

・端末が持つ物理機能ブロック（例 通信インタフェースカード、CPU、メモリ）に何があるか。
・端末が持つ論理機能ブロック（例 VLAN等の論理通信インタフェース、DVD内蔵型TVにおけるDVDプレイヤー機能とTV機能）に何があるか。
・論理機能ブロックの設定情報（例 論理通信インタフェースに割り当てられたIPアドレスやDNSサーバのIPアドレス）。
・端末間の接続情報。（例 MACアドレスAの端末xが、論理通信インタフェース1に接続している）

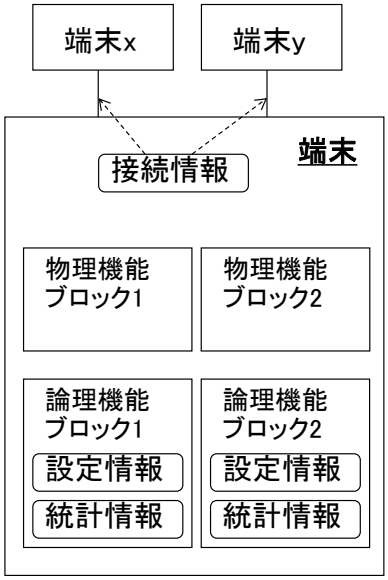

図3-3. 端末と構成情報、統計情報の関係

構成情報取得機能を実現する既存プロトコルの例として、TTC HTIP「ホームNW接続構成特定プロトコル」（TTC JJ-300.00, ITU-T G.9973）、LLDP（Link Layer Discovery Protocol）、UPnP Forum UPnP（Universal Plug and Play）、IETF SNMP（Simple Network Management Protocol）が挙げられる。

(2) 統計情報取得機能

統計情報取得機能は、カスタマサポート対象となるシステムを構成する、ネットワーク機器を含む各端末の稼働状況に関する情報を取得する機能と定義する。統計情報の例として、以下のものが挙げられる。（図3-3）

・論理通信インタフェースにおける送受信パケット数、廃棄パケット数。
・ビデオコーデック機能を実現する論理機能ブロックにおけるフレーム再生失敗数。
・端末の起動時刻や連続稼働時間。

統計情報取得機能を実現する既存プロトコルの例として、IETFで標準化されたSNMPが挙げられる。

3.3.2 低位レイヤ負荷試験

本節の低位レイヤは、レイヤ2（イーサネット等）、レイヤ3（IP等）、レイヤ4（TCP、UDP等）のことと定義する。低位レイヤ負荷試験は、HNを構成する端末間の通信に対して低位レイヤのトラフィック負荷をかけることで、端末自体の通信処理、もしくは、端末間を接続するネットワークに問題が無いかを確認するために利用可能である。

低位レイヤ負荷試験のために、パケット（レイヤ3）またはフレーム（レイヤ2）レベルの試験用トラフィック処理機能が必要となる。試験用トラフィック処理機能実現のため、HNを構成する端末（の一部）に、以下の2つの機能が必要となる。（図3-4）

・試験用トラフィック送信機能
　カスタマサポート対象となるシステムを構成するネットワーク機器を含む各端末から、別の端末に対して、パケットを試験に必要なトラフィックパターンで送信する機能。
・試験用トラフィック受信機能
　試験用トラフィックを受信する側の端末に、試験用トラフィックを受信し、どの程度受信できているかを調べるための機能。

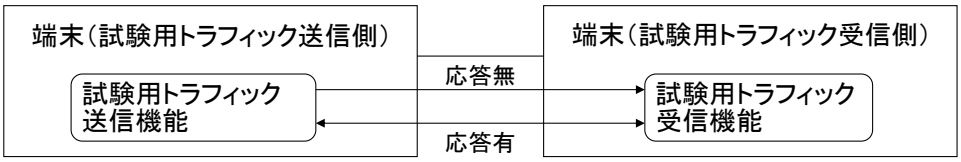

図3-4　試験用トラフィック処理機能の実現構成

試験用トラフィック処理機能の実現方法として、以下の例が挙げられる。

・試験用トラフィックとしてping（ICMP ECHO Request）を用い、受信側端末が送信側端末に応答を返すことで確認。試験用トラフィック送信機能、試験用トラフィック受信機能として、特別な機能追加が不要となる可能性がある利点がある。一方、レイヤ4に依存した問題（例　TCPの処理能力不足）が検出できない欠点がある。
・試験用トラフィックとして受信側端末が受信処理可能なパケットを使用し、受信側端末の統計情報取得機能を利用して、試験用トラフィックの処理状況を確認。試験用トラフィック送信機能の機能追加が必要となるが、試験用トラフィック受信機能は特別な機能追加が不要となる可能性がある利点がある。

・専用の試験用トラフィック送信機能と試験用トラフィック受信機能を追加。追加機能の開発量は増える欠点があるが、VoIP用パケットの受信ジッタ測定等、サービスに合った試験を実現できる利点がある。

HNを構成する端末の中で、試験用トラフィック生成機能を持つものが多い程、HN内で低位レイヤ負荷試験対象にすることができる範囲が広くなる利点がある一方、低位レイヤ向け負荷試験のための機能追加による端末のコストアップといった課題も存在する。試験可能な通信経路に制限が生じるが、試験用トラフィック送信機能を、HGWの様に処理能力に余裕がある装置にのみ搭載するケースも考えられる。

低位レイヤ負荷試験に必要な機能を実現可能な既存ツールの例として、以下のものが挙げられる。

・ping flooding：pingコマンドのオプションで、ECHO Replyを待たずにECHO Requestを送信。
・Ethernet OAM：ITU-T Y.1731で標準化された、Ethernet網の保守管理機能。例えばEthernet OAM LB（Loop Back）でpingと同様の導通確認が可能。
・iperf：TCP、UDPのパケットで負荷試験を実行可能なフリーソフトウェア。試験用トラフィック送信機能と試験用トラフィック受信機能の両方を実現する。

負荷試験を実施する以前に、低位レイヤでの導通性確認を行うことが必要になる場合も考えられる。レイヤ3の導通性確認の目的には、ICMP ECHO Request/Replyを利用したpingコマンドやtracerouteコマンドが利用可能である。レイヤ2の導通性確認の目的では、Ethernet OAMのEthernet OAM LB（Loop Back）やLT（Link Trace）が利用可能である。

3.3.3　アプリケーションレイヤ負荷試験

アプリケーションレイヤ負荷試験は、アプリケーションレイヤのトラフィック負荷をかけることで、端末のデータ処理、もしくは、端末間を接続するネットワークに問題が無いかを確認するために利用可能である。

アプリケーションレイヤ負荷試験のために、アプリケーションレベルの試験用トラフィック送信機能が必要となる。試験用トラフィックの受信機能は、実サービスで使用するアプリケーションに行わせることを想定する。（図3-4、図3-5）

・試験用トラフィック送信機能が被試験対象端末（試験用トラフィック受信側端末）と別端末に存在し、ネットワークを介して試験用トラフィックを転送。

　アプリケーションレベル（実際のアプリケーションが使用する映像、音声、センサデータ等）の試験用トラフィック生成機能を、HGWの様に処理能力に余裕がある装置に搭載し、被試験対象端末へ送信する。（図3-5）

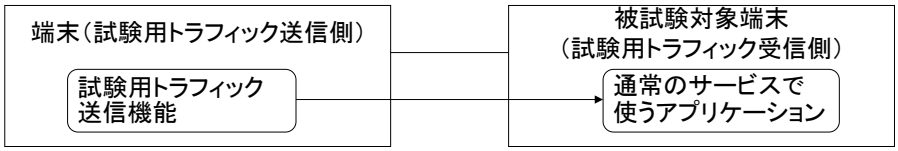

図3-5　試験用トラフィック送信機能が被試験対象端末と別端末に存在するケース

・試験用トラフィック送信機能が被試験対象端末（試験用トラフィック受信側端末）と同一端末に存在し、端末内部で試験用トラフィックを転送。

　アプリケーションレベル（実際のアプリケーションが使用する映像、音声、センサデータ等）の試験用トラフィック生成機能を、被試験対象端末内部に実装する。（図3-6）

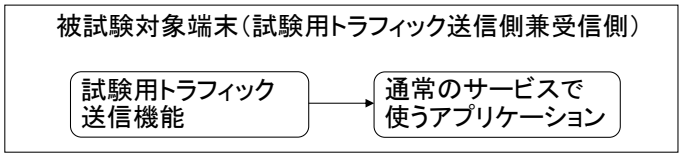

図3-6　試験用トラフィック送信機能が被試験対象端末に存在するケース

アプリケーションレイヤ負荷試験においては、統計情報取得機能で、アプリケーションでのトラフィック処理状況を確認できることが望ましい。しかし、映像配信サービスの様に、ユーザがサービス品質を自分の五感で判断できる場合、統計情報の様な定量的指標が無くても良い場合も有り得る。

3.4　WAN での課題を解決する機能

本節では、WANとHNの通信について、その通信品質低下の要因がWAN側にあるケースを想定したときに、カスタマサービスに求められる機能を3.4.1～3.4.2で説明する。また、3.4.3では接続状態と接続試験、3.4.4では利用可能帯域の測定手法とサービス間の調整のための帯域制御に関する方法論について説明する。なお、通信事業者の設備障害等はカスタマサポート対象外とした。

3.4.1　ネットワークレイヤ競合チェック

ネットワークレイヤの競合については、(1)通信方式間の干渉や漏洩電波によるサービスへの影響と、(2)ネットワークリソース（通信帯域）の競合の2つの課題がある。

(1)通信方式間の干渉やサービスの競合

携帯端末の発展普及を背景に、家庭においても複数の放送・通信サービスを利用することが一般的になってきた。放送・通信については各方式間で信号の干渉や漏洩電波に関する課題が存在し、サービス事業者はサービス提供時に適切な説明を行う義務が課されているが（放送法150条、電気通信事業法26条）、利用中のサービスに加え別途新しいサービスを利用する場合や、サービスの乗り換えの際には、ユーザ自らがサービスの提供条件を理解したうえで、その利用可否を判断しサービス事業者と調整を行わなければならない。しかし、ユーザの多くは通信や放送に関する技術的な知識が少ないのが実情であり、そこでトラブルが発生する可能性がある。

干渉や漏洩電波に関する問題についてはサービス事業者や機器メーカによって技術的な課題解決が常に行われているが、一般家庭の傾向として、旧方式の機器であっても利用できる限りは使い続けることが多い。そこで技術的な課題のある機器が残存することが想定される。こうした設置機器等の情報の管理についても課題となるだろう。さらに、有線系のサービスの場合は宅内の既設配線の利用状況（配管、構内配線または宅内配線の線番情報）を把握し、先行するサービスへの影響に配慮することが必要である。設備情報や配線経路の情報についても、ユーザや建物所有者側での管理者不在のケースもあり、通信品質の確保と円滑なサービス提供のためにもこうした設備関連の情報管理が望まれる。無線系のサービスについては電波干渉などのトラブル履歴など建物ごとに管理することが有効と思われる。

これらの課題に対するカスタマサポートとしては、ユーザが利用している機器やサービスについて、通信方式間の干渉やサービスの競合をチェックできるよう、情報管理の支援または補完を行い想定されるトラブルの回避、またはその影響を軽減することが期待できると考える。

(2)ネットワークリソースの競合

次に、アクセスネットワークの帯域の制約に起因する問題（いわゆる「ふく輳」）について説明する。

HNに関して外出先からインターネットを利用してHN内の端末を操作するという利用シーンが広く認知され、さらにWANからHNに提供されるクラウドサービス（ex.ビデオストリーミング、ネットワークゲームなど）の利用も着実に増加しつつある。このようにHNの利用が高度化し接続される端末が増えるにしたがいWANとの通信量の増加が予測される。先の例のような利用シーンではWANを経由して行う操作性やクラウドサービスなどの利用品質は通信品質（遅延、パケットロス、揺らぎ）の影響をうけるため、問題が発生した場合はカスタマサポートが求められると想定する。

そこでカスタマサポートとしては、はじめに通信状態を把握することが必要となるだろう。HNとWANの通信量については、HGWには送受信のパケット数、廃棄フレーム数、受信合計バイト数、遅延時間などの統計情報（転送パケット数、破棄数、エラー数）等、以下のようなトラフィック処理の統計情報機能が求められる。こうしたトラフィック処理の統計情報についてはHGWの処理に負担がかかるため実装においてコスト面が課題になると思われる。またこうした情報の取得方法としてはSNMP（設定情報、統計情報）、BBF TR-069（設定情報）の機能を活用することができる。

3.4.2　アプリケーションレイヤ競合チェック

HNの利用の高度化は端末の遠隔操作にとどまらず、クラウドの潤沢なリソースを利用することで様々な情報やサービスとの連携が可能となり、エコで快適な端末の設定や複数端末のシーケンス制御、自動調整が可能になる。一方でこうした利用シーンを考えた場合に、端末に対する宅内の操作とクラウドサービスの制御指示が競合するようなケースや、HN内にいるユーザ自らの指示とは異なる指示をおこなってしまうケースが想定される。具体的な例でいうと、室温設定について競合するサービスが各々のプログラムに基づいて室温20度設定と18度設定の指示を交互に繰り返すケースや、照明器具のON/OFFを繰り返してしまうという事象が典型的なケースである。こうしたサービス間の競合は、各々がいわば正常な操作、制御であるがゆえに相互で調整し判断するのは困難なケースが多い。こうした課題の解決についてはユーザの意向や判断に加え、安全性の観点から各サービス間を調停する機能が求められる。

(1)課題解決

カスタマサポートによる課題解決のためには、家庭内の状態監視、各サービス間の調停機能や安全の観点で一方のサービスの停止を行うためのユーザとの事前合意やルールづくりが必要だろう。

本技術レポートの前提としては3.4.1に説明したのと同様に利用しているサービスの情報や現在のHNの状態を把握したうえで、ユーザとの対話を通じて課題解決することが考えられる。

管理手段・実現方法としては前述のとおり宅内のHNの状態参照はECHONET（接続端末発見、端末情報、状態参照）、TTC HTIP（接続端末発見、端末情報、トポロジー把握）が利用できる。ただしこれらのプロトコルはリンクレイヤブロードキャストドメインに限られるため、リモートからこれらの情報を取得するには、例えばBBF TR-069（設定情報を遠隔から取得）を前提に情報を遠隔から取得するための機能をHGWに実装する必要がある。ネットワークレイヤのSNMP（設定情報、統計情報を遠隔から取得）の活用も考えられる。

(2)ユーザ管理主体性の維持

本課題に関連する問題として、HN内においてクラウドと連携した分散協調型サービスの利用が一般化する段階では、ユーザが個別具体的に認識してないアプリケーションが端末にインストールされるケースや、端末の設定が自動で変更されてしまうケースについて、もっともプライベートな空間のHNにあってこうした状況を望まないユーザや自己の管理下におきたいというユーザも存在すると思われる。

そこで、そういうユーザの要望に配慮して、導入されているソフトウェアや端末情報など、HN内の構成管理を行うことが必要になるだろう。そのためには、外部のネットワークにつながるHGWを通過するトラ

フィック（フレーム）を分析して不審な通信が行われていないかを監視する機能（DPI：Deep Packet Inspection）や特定のアプリケーションの利用を遮断する機能（フィルタリング：filtering）などの実装についても検討が必要であろう。

3.4.3　接続状態

3.4.1と3.4.2ではネットワークレイヤとアプリケーションレイヤに分けて、想定される不具合に対するカスタマサポートと、そこで必要となる機能について説明をしてきた。以下の3.4.3、3.4.4ではそれらに共通したプラットフォームに必要な保守機能や試験の方法について説明する。

(1)導通確認

導通試験について、WANのプロトコルは通信事業者が利用する前提で試験機能も組み込まれており、それらの機能の利用が考えられる。しかし、HNとアクセスネットワークの接続形態により慎重に整理する必要がある。HGWの位置づけを事業用通信設備とするか端末設備とするかで責任分界点も異なるため、本レポートでは課題を指摘するのみにとどめる。仮にTCP/IPでいうところのリンクレイヤ以下のレイヤの導通試験を行うとした場合、アクセスネットワークの通信方式の多様性はカスタマサポートの課題となるだろう。常に新しい方式に対応する必要があるとともに古い規格への対応継続が課題となる。

EthernetについてはEthernet OAM（ITU-T Y.1731、IEEE802.1ag）、またATMにはATM OAM（ITU-T I.610）を利用することが想定される、また一般的なインターネットアクセスで利用されるPPPoEやPPPoAはPPPのLCPを利用することが想定される。

ネットワークではICMP（IETF RFC792、IETF RFC4443）のEcho要求、いわゆるPing試験が有効である。TCPについてはTelnet（IETF RFC854）を利用することができる。

(2)遅延測定

ネットワーク層のICMP（IETF RFC792、IETF RFC4443）の利用が有効である。

(3)状態参照

接続障害の状況が継続的ではなく、一時的または断続的な状況においては、HGWの統計情報等を活用して状況把握を行い、保守対応を検討することが有効だろう。そのためには通信履歴（リンクアップ時刻、リンクアップ時間、トラフィック量、各種アラーム）、統計情報（廃棄フレーム数、エラー数）などのログの取得が必要となるだろう。

3.4.4　帯域制御

(1)通信品質測定について

HNに接続するアクセスネットワークやさらに上位のインターネットについてもいわゆるベストエフォートのサービスであり、利用者の環境次第で通信品質が異なるのが実情である。そこでユーザ環境ごとに利用可能帯域を把握する機能が必要となるだろう。

利用可能帯域測定の手法としては、パッシブ測定とアクティブ測定がある。パッシブ測定はユーザの実トラフィックを分析対象として利用可能帯域を推定する手法だが、ユーザトラフィックに依存するため精度面での課題がある。他方、アクティブ測定は、評価用のトラフィックを実際に送信してその処理状況から利用可能帯域を推定する手法だが、評価用のトラフィックが利用中のサービスに影響を及ぼす可能性がある。

アクティブ測定の方式例としては、PPDP（Packet Pair or Train Dispersion）、VPS（Variable Packet Size）、SLoPS（Self -Loading Periodic Stream）、TOPP（Train of Packet Pairs）などがある。

これらのアクティブ測定手法でもサービス影響が許容されるカスタマサポートの対応局面では有効に利用できる可能性がある。またアクティブ測定でもネットワークへの負荷が軽微なインラインネットワーク測定手法としてImTCP（Inline measurement TCP）など注目すべき研究報告がある。

(2)帯域制御について

3.4.1でHGWの統計情報を確認し、前項で残余帯域が把握された後、実際に是正措置を行うことが求められるが、比較的広帯域のHNから、比較的帯域に制約があるWANに向けて送出されるトラフィックがHGWを通過するポイントがボトルネックになるであろう。

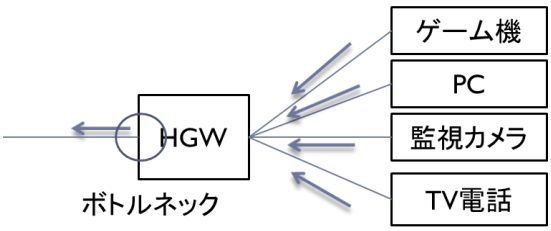

図3-7. HN~WAN通信のボトルネック（上りトラフィック）

そこでHGWにおいて輻輳が発生した場合、各端末から受信するトラフィックの優先度付けが問題となる。

本課題についてはTTC TR-H.QoS(Sup11) 「クラス型ホームネットワークQoS技術の分析」において、「ホームネットワークQoS技術調和のための枠組み」が示されている（図3-8、3-9）。

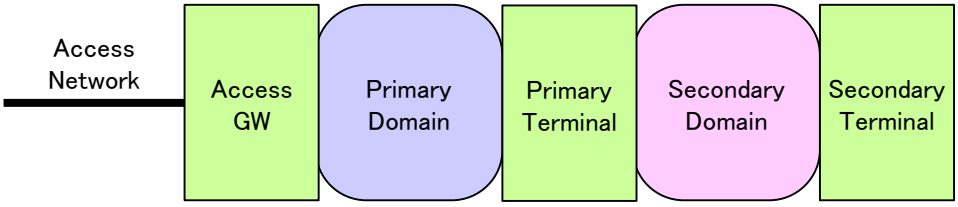

図3-8. ITU-T H.622で規定されたホームネットワークのアプリケーションモデル

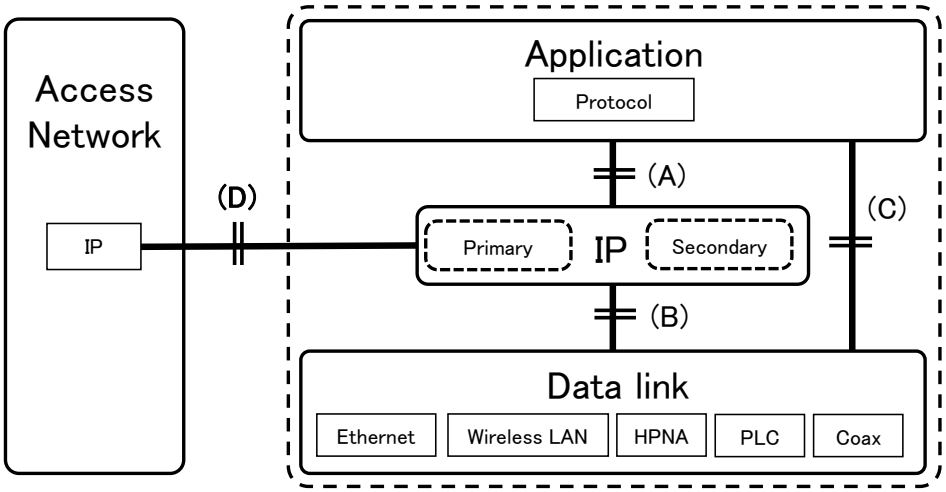

図3-9. ホームネットワークQoS技術調和のための枠組み

TTC TR-H.QoS(Sup11)では、QoSを調整するため4つのインタフェースを定義し、優先度レベルやマーキングの運用について各標準化団体の文書を分析し、QoS技術の整合の方向性を検討したものだが、A、Bの各インタフェースはHN内に閉じた通信を対象としている関係で多くの標準化段階で検討されている一方で、

WANとHN間の通信に関するインタフェースDについては言及している文書が少ない（TTC TR-H.QoS(Sup11) P9）。

利用者の利用形態の高度化にともない、各標準化団体相互で調整がおこなわれるだろうが重要通信確保の観点も必要になるだろう。

これらの調整を前提に、カスタマサポートの対応のためHGWには帯域制御（優先制御）機能が必要になるだろう。加えて、HGWは各端末から送出されるトラフィックについて帯域の割当を行うために、その優先度を識別する、各端末は送出するフレームやパケットにその優先度付けのマーキングを行う機能が必要になる。

3.5　サービス干渉を解決する機能

3.2～3.4節では、端末、HN、WANの設定やトラフィック、無線干渉などのトランスポートレイヤ以下の原因の特定方法について記載した。3.5～3.6節ではアプリケーションレイヤでの原因の特定方法について述べる。

アプリケーションレイヤにおける原因としては、サービス干渉が考えられる。たとえば、障害事例の項目5では、HNに接続されるNAS（Network Attached Storage）に記録されるビデオデータをPCで専用アプリケーションを使って再生しようとすると、通信が遮断されてPCで再生できないという事例が紹介されている。この原因は、このPCで動作している別のアプリケーションの不具合で、PCが受信したビデオデータが欠損するためであった。このように、HN上に接続される端末の機能やPCのソフトウェアの組み合わせにより障害が発生する可能性がある。

この課題に対する解決方法としては、図3-10のようにHNに接続される端末情報のほかに、端末上で動作するアプリケーションや機能（ハードウェア）のリストを作成し、同時に動作させることで障害になりうるアプリケーション・機能の組み合わせを管理する必要がある。しかし、この組み合わせの情報は、経験的にしか得られないものである。したがって、この競合するアプリケーションの組み合わせをデータベースとして蓄積し、HN内に設置される端末やインストールされるアプリケーションの組み合わせをチェックしていくことが解決策と考えられる。

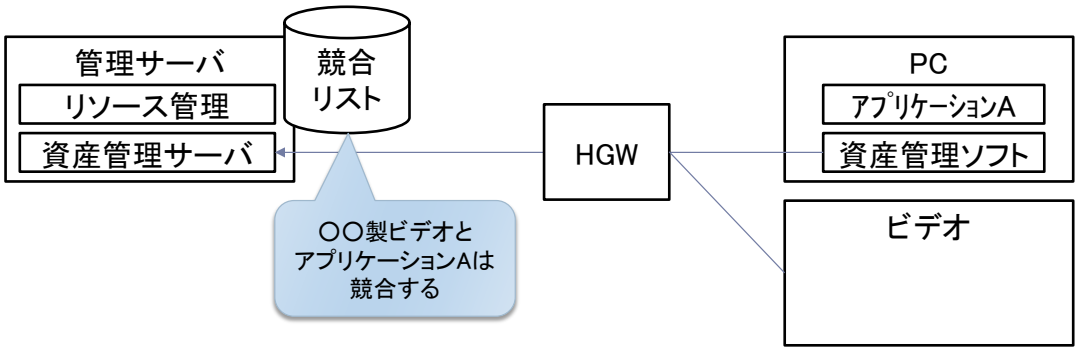

図3-10 競合サービスチェック機能の実現アーキテクチャ

図3-10は、HNに接続されるアプリケーションの競合関係をチェックするためのアーキテクチャを示している。HN内に接続される家電や、PCやスマートフォンのような汎用OSで動作する端末が接続される。PC内で動作するアプリケーションの情報は、インストールされているアプリケーションを検出する資産管理ソフトウェアが検出する。一方、クラウド側では管理サーバでHNに存在するリソースを管理するトータル情報管理機能がある。家電の情報は、接続時にECHONET Lite等のプロトコルにより端末情報を取得するが、PCのような汎用OSで動作する端末は、3.2.4で述べた資産管理システムを利用して取得する。具体的には管理サーバ上で資産管理サーバが動作し、PCの資産管理ソフトウェアと通信して、インストールされているアプリケーション情報を取得する。この情報をリソース管理機能で他の端末情報と併せてリスト化する。一方で、リ

ソース管理機能は、競合関係があるアプリケーションや機能（端末）の組み合わせデータベースに照会を行って、干渉するアプリケーション等を発見する。

3.6　ユーザ誤操作による障害解決機能

ユーザ誤操作による障害は、システムは正常に動いているが、ユーザの勘違いや操作ミスにより、ユーザの所望の動作とは異なる動きをするために、ユーザが障害と認識してしまうケースを指す。たとえば、バイタルセンサ（血圧や体温等の生体情報を測定するセンサ）を身に着けて病後の監視を行うようなサービスでは、患者がセンサを付け忘れることにより異常と検知されるケース。このケースは、システムは正常に動いているが、得られるデータが異常値を示すために障害とみなされる。または、操作A、操作B、操作Cと3つの操作をすべきところで、操作A、操作Cと操作Bを省いてしまい、最後の操作Cを行った後の端末やサービスの動作がユーザの想定していた動きと異なるケース。このケースもシステムは正常の動作をしているが、ユーザは操作Bをし忘れたことに気づかない限り、システムが正常に動いていないと判断してしまう。

この問題の検出に関しては、決まった解決方法は確立されていないが、ユーザ操作が通常とは異なることをユーザに通知する方法が必要である。以下のような検出方法が考えられる。

(1) ルールベースによる検出

端末やアプリケーションの内部状態とユーザ操作の履歴を保存し、内部状態と操作との関連から判断する方法が考えらえる。実際の操作を行う上で、経験的に起こりにくい操作と内部状態との関係をルール化し、このルールに合致する操作が発生したときに、その記録を残す。ユーザから障害として報告されたときに、この履歴を確認してユーザ誤操作かシステム障害かの切り分けを行う。

(2) 統計処理による検出

端末やアプリケーションの内部状態とユーザ操作の履歴を保存し、内部状態と操作の時系列データから通常時の操作と内部状態との時系列パターンを生成する。ユーザから障害として報告されたときに、この通常の操作パターンに合致するかどうかでユーザ誤操作かシステム障害かの切り分けを行う。

第4章　システム技術要件

HNでは複数のシステムが同時に動作し、多くの小さな問題が発生している。この状況がHNにおける障害復旧を難しくしていると考えられる。3章では、個々のリソース、すなわち、端末（端末ハード）、サービス（端末ソフトウェア、アプリケーション）、ネットワークにおいて取得すべき情報や復旧プロセスを支える機能について述べた。4章では、同時に発生する問題、参照すべき情報を一元管理し、コールセンタ等のサポートを行う事業者、または部門が遠隔サポートするときに必要となる情報を提供する仕組みについて説明する。

4.1　概要

HNサービスでは、端末を設置する住宅等にシステム管理者が不在であり、遠隔から管理することが前提になっている。しかし、従来の電話によるサポートでは、HN内で発生している状況を正確に把握することが困難であり、障害からの復旧が困難であった。障害が発生した際には、HNに接続されている端末の情報、HNのトポロジー情報、トラフィック情報、PCやスマートフォン等で動作するアプリケーションなどの情報を取得したうえで、原因を分析する必要がある。特に、最近のHNは接続される端末も増え、原因も複雑になっているため、動かない端末の情報のみを得られたとしても原因特定できない場合が多い。したがって、遠隔からのサポートを行うには、従来ユーザからのヒアリングでは得られなかった詳細の情報を取得し、ある程度集約して分析を行えるような仕組みが必要となる。

図4-1は、遠隔サポートで必要となる基本機能構成である。このアーキテクチャでは2つの機能について示している。ひとつはHN内の端末やネットワークの設定を遠隔から確認、変更するための機能。もうひとつは、HN内の端末やネットワークの内部状態やトラフィック情報をリアルタイムに収集する機能である。以下、簡単に図を説明する。端末にあるManaged Agentは、端末内の設定情報や内部状態を管理し、外部から設定変更があれば端末内部の設定を変更するAgentである。HNにあるWiFi AP（Access Point）やルータ等については、ネットワークのトラフィックや設定情報を管理、問い合わせに応じて返信する機能が備わっている。HGWでは、端末やネットワーク機器の設定を行うConfiguratorや内部情報やトラフィック情報を集約するResource information collectorがある。管理PFでは、設定情報等の静的な情報と内部状態等の動的な情報をResource managementが管理する。アプリケーションには、カスタマサポート向けのアプリケーション（Management application）と一般のアプリケーション（Service application）が存在する。Management applicationは、エンドユーザからの障害問い合わせに対して、ユーザ宅のHNや端末の状態を表示したり、必要に応じて設定を変更したり、試験用のトラフィックを発生するなどの操作を行う。Management applicationから実行可能な操作は、3章で述べた障害の原因分析や復旧を行う各機能を操作することで実現される。

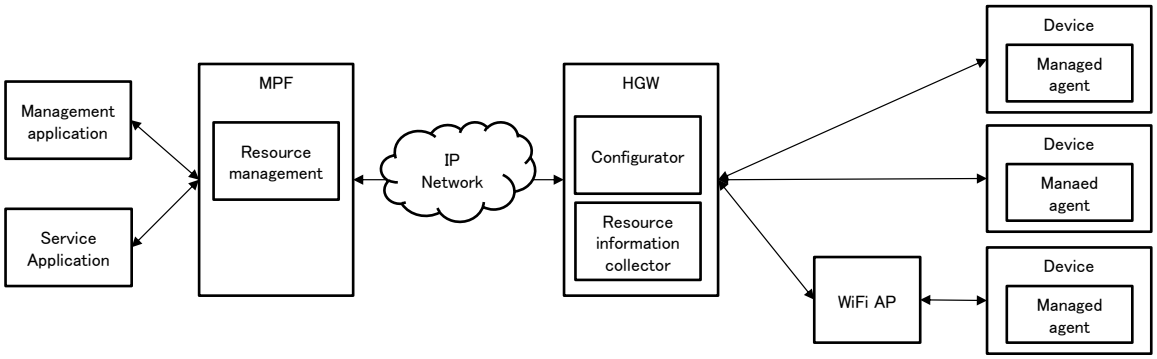

図4-1 遠隔サポートのためのフレームワーク

デバイス管理に機能は限定されるが、BBF TR-069は同じアーキテクチャで遠隔での端末の設定やファームウェアのアップデートなどの機能を持っている。また、最近の規格では、HNに接続されるリソースを遠隔から管理するISO/IEC 30100が規格化されている。ISO/IEC 30100では、リソース管理としてHNに接続される端末だけなく、ネットワークやソフトウェアの管理も行う枠組みになっている。当面は、BBF TR-069等のすでに普及している規格を拡張する実現方法も考えられるが、将来はISO/IEC 30100のような枠組みが広く普及することも予想される。

4章の以下では、ISO/IEC 30100と関連する規格について説明する。

4.2　ISO/IEC 30100

ISO/IEC 30100は2013年に制定された規格であり、HNリソース管理に関するものである。この規格では、HN内のリソースとして、位置情報（設置位置）、デバイス情報（内部機能状態）、ネットワーク情報、サービス情報をリソースとして定義している。これらの情報はHNからインターネット上に存在するHNリソース管理機能で集約をし、管理アプリケーション（Management Application）からその内容を参照するようになっている。管理アプリケーションは、コールセンタや保守作業者が参照し、ユーザの障害復旧の支援を行ったり、遠隔から端末（端末、ネットワーク機器）の設定を変更するなどして遠隔から復旧作業を行ったりする。

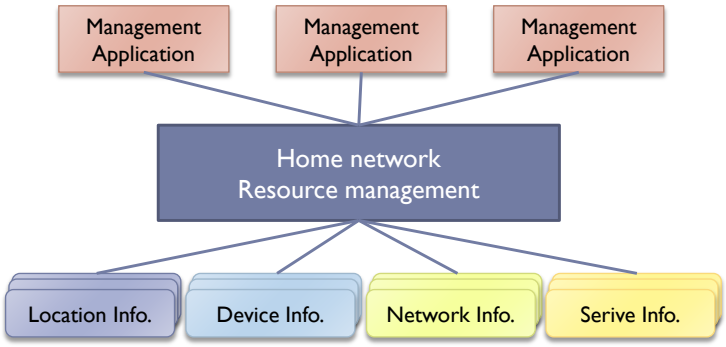

図4-2.　HNリソース管理モデル

また、リソース間の関係を定義することができるようになっており、障害発生時に関係情報を元に関連する情報を参照することができる。

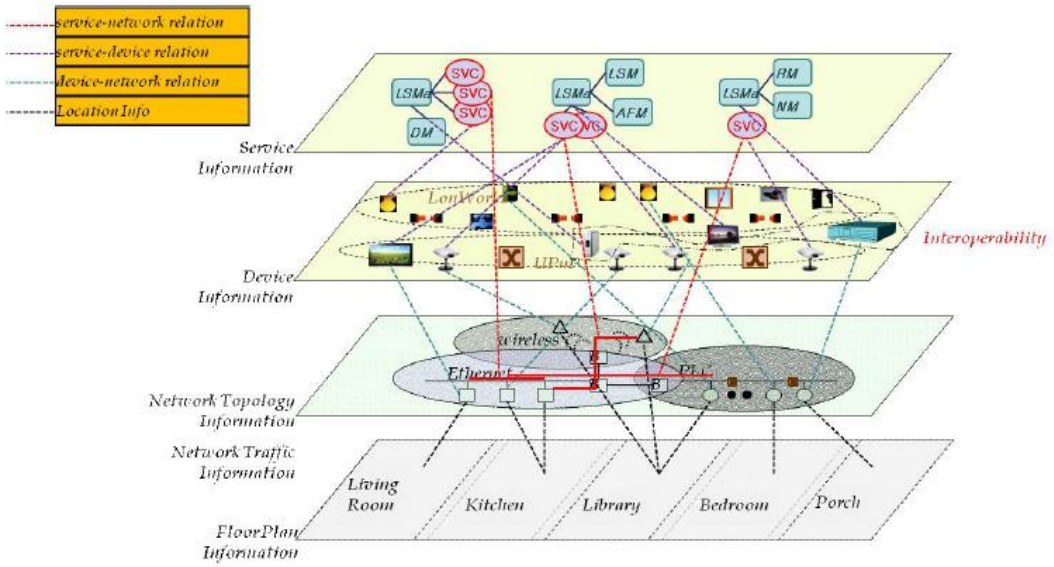

図4-3.　HNリソース管理アーキテクチャの論理概念

なお、ISO/IEC30100では、例として、位置情報はBuilding Information Model (ISO/PAS 16739)、端末情報はKNX (ISO/IEC 14543-3シリーズ)、ネットワーク情報はSNMP (RFC 1098)、サービス情報はOSGi (OSGi Alliance)を参照している。

4.3 関連規格

4.3.1 IEC 62608

IEC 62608は、TC100委員会で標準化がすすめられている規格であり、HNに接続される端末の各種の設定を行うための参照モデルになっている。規格は、Part 1～3からなっており、現在、Part 1が承認されている。

IEC 62608では、図4-4のようなモデルで構成される。ConfiguratorはHNに接続される端末が動作するために必要な設定を行うものであり、端末に存在するConfigured Agentが設定すべき項目をConfiguratorに送信すると、必要な設定情報をConfiguratorが返信するようになっている。

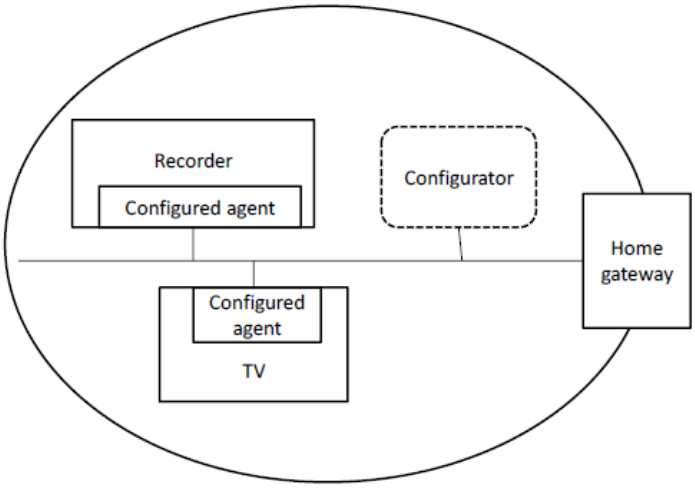

図4-4. Configurator system model

ConfiguratorがAgentに応答する情報をインターネットで管理する方法については、G.9980（TR-069）を使用することを検討中である。

4.3.2 G.9980（BBF TR-069）

G.9980は、BBF TR-069を参照する規格である。BBF TR-069は、HNに接続される端末（CPE: Customer premises equipment）をインターネットから管理するプロトコル（CPE WAN Management Protocol）である。図4-5は、BBF TR-069のアーキテクチャを示したものである。端末は、ゲートウェイ（Managed Internet Gateway Device）を経由してWANに接続されており、WAN上にある設定サーバ（ACS: Auto-Configuration Server）に接続される。ACSは、HNに接続される端末の設定情報を保持しており、端末が接続されるとその設定情報が通知されたり、必要なファームウェアをダウンロードすることができる。図中、ACSの左側（Northbound interface）には、コールセンタ等が接続され、エンドユーザからの問い合わせがあったときなどに、このインタフェースを利用して設定情報を参照する。

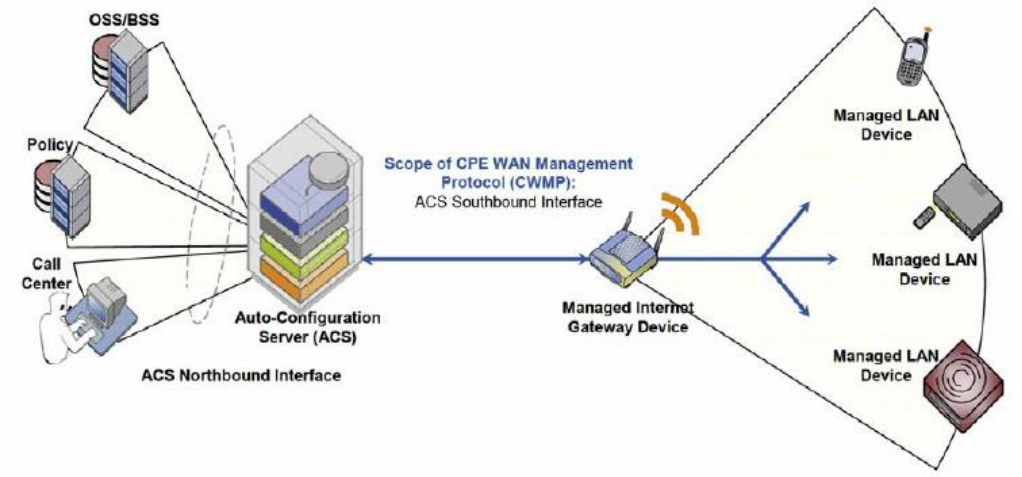

図4-5.　BBF TR-069の構成

4.3.3　UPnP DM

UPnPは、UPnPフォーラムで策定された規格であり、端末がネットワークに接続されたときに自動的に設定がされ、使用可能になるための基本的な仕組みを規定している。UPnP DMは、UPnPを利用してデバイス管理を実現する規格である。図4-6は、UPnPのデバイス管理の仕組みを示したものである。

UPnP Manageable Deviceは、LAN IPで接続される端末である。設定可能な情報はDevice data modelとして規定される。UPnP Control Point（CP）は、UPnPプロトコルを使用してUPnP Manageable Deviceの設定を行う。UPnP CPで保持される設定情報は、WANを経由してクラウドで管理可能である。

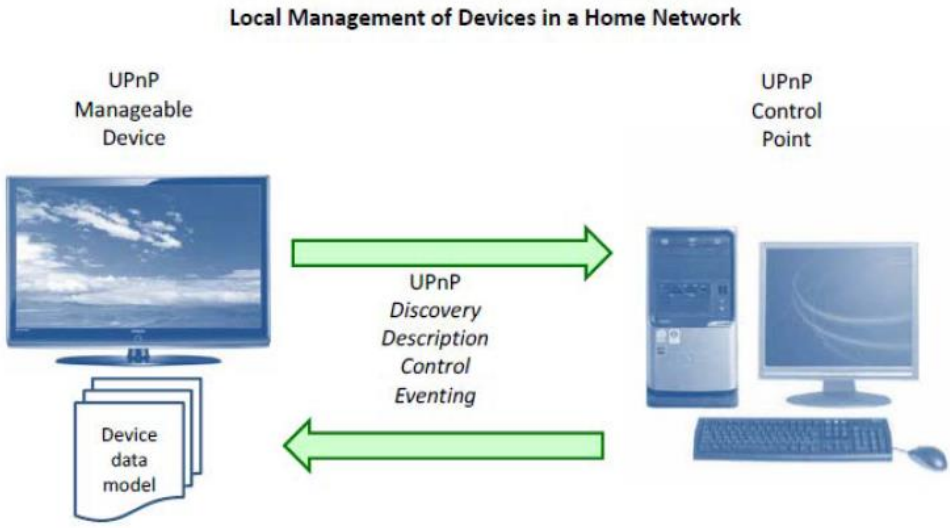

図4-6.　UPnPによるデバイス管理

4.3.4　OSGi RMP

OSGi（Open Service Gateway initiative）フレームワークは、モジュールからなるシステムであり、Javaプログラミングされたコンポーネントを動的に導入することが可能なサービスPFである。コンポーネントは、バンドル（Bundle）と呼ばれ、システムを再起動することなく、インストール、起動、停止、アップデート、アンインストールができるようになっている。バンドルを制御する遠隔管理プロトコルが規定されており、HN端末を管理するために利用される。

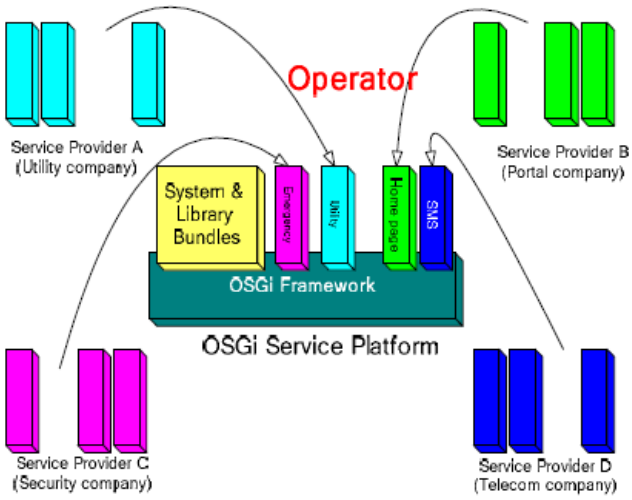

図4-7　OSGi remote management protocol

4.3.5　OMA DM

OMA（Open Mobile Alliance）は携帯電話事業者向けのオープンな仕様である。この仕様は、国、事業者、端末に関わらず共通なサービスイネーブラを提供することを目的としている。OMA DMは、携帯電話やスマートフォン、PDAのような携帯端末を管理するためのデバイス管理プロトコルである。

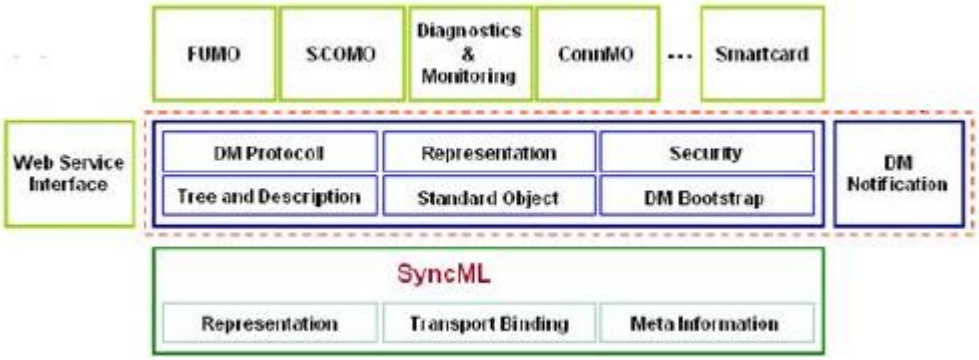

図4-8.　OMA DM protocol stacks

4.3.6　SNMP

SNMP（Simple Network Management Protocol）は、IPネットワーク上の端末を管理するインターネット標準プロトコルである。SNMPをサポートする端末は、ルータ、スイッチ、サーバ、プリンタなどがある。ネットワークに接続可能な端末をモニタするための管理システムであり、ネットワーク管理者に状況を伝えることが目的である。ネットワーク管理の標準的な機能からなるが、アプリケーションレイヤのプロトコルやデータベース、データオブジェクトが規定されている。

第5章　ビジネスモデルとアーキテクチャ

5.1　ビジネスモデル

本節では、HN・カスタマサポートに対応したサービスプラットフォームを利用するビジネスモデルの想定について説明する。想定される事業形態として、中間事業者型、クラウドサービス事業者型、サービス売り切り型の3つが考えられる。以下に、3つの事業形態を説明する。

(1) 中間事業者型

サービスプラットフォームを提供する中間事業者が全ての情報を管理し、サービス事業者やサポート事業者に対してAPIを提供して、必要な情報のやり取りを行う形態。（図5-1）

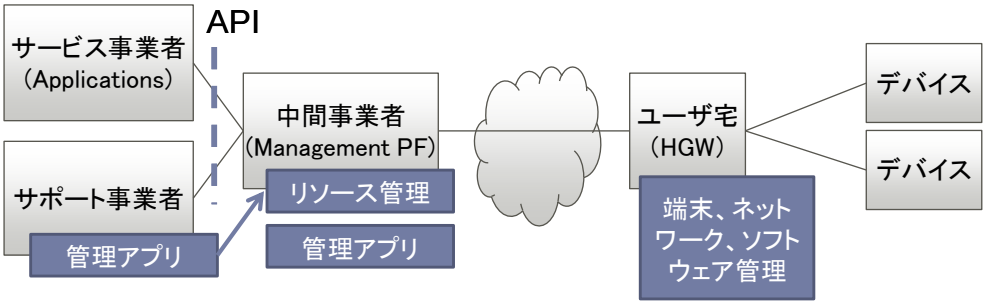

図5-1　中間事業者型

図5-1における端末、ネットワーク、ソフトウェア管理は、ユーザ宅内の個々の端末の情報収集と制御を行うための機能を提供する。リソース管理は、各ユーザ宅が提供する情報と制御の機能を統合し、データベース等情報管理の機能も提供し、APIとして提供する。管理アプリは、リソース管理がAPIで提供する機能を利用し、カスタマサポートサービスのための機能（例 障害原因特定、障害回復措置実行）を実現するアプリケーションである。端末、ネットワーク、ソフトウェア管理、リソース管理、管理アプリの役割は、これ以降で説明するクラウドサービス事業者型やサービス売り切り型でも同じである。

(2) クラウドサービス事業者型

サービス事業者が主導的に事業をまとめ、端末保守をサポート事業者に委託する形態。（図5-2）

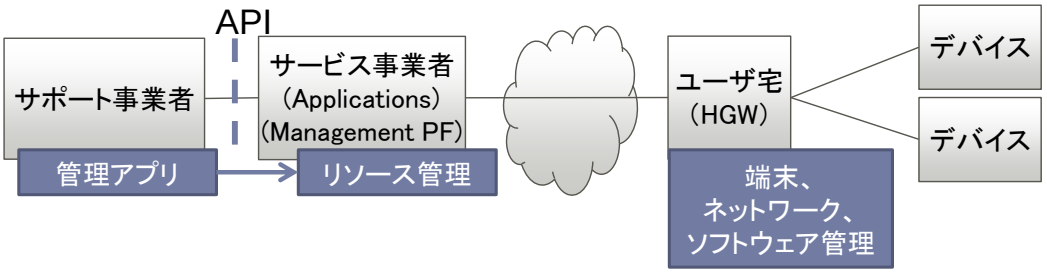

図5-2　クラウドサービス事業者型

(3) サービス売り切り型

中間事業者やサービス事業者を介さず、サポート事業者が直接ユーザ宅に接続する形をとり、リソース管理機能までをユーザ宅に配置する。この場合、簡易管理アプリまでユーザ宅に配置し、ユーザが自力で解決できないトラブルのみサポート事業者が対応するという形態も考えられる。（図5-3）

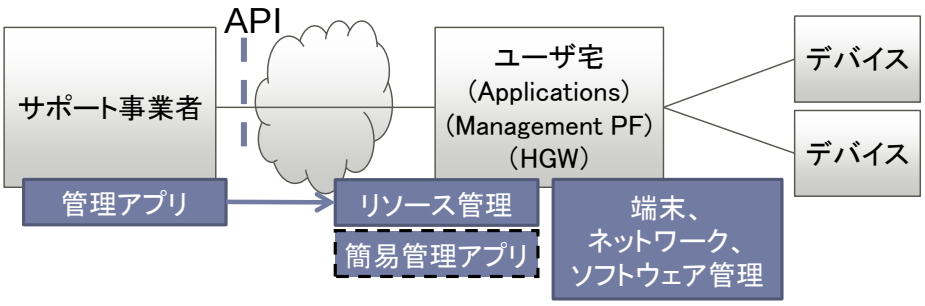

図5-3　サービス売り切り型

5.2　ケーススタディ

本節では、ユースケースに基づいてここまで述べたカスタマサポート機能の動作を説明する。エンドユーザもしくは代行者が、HNサービスの利用登録、端末の設置を行い、HNサービスの利用開始後、障害が発生して復旧にいたる手順について解説する。なお、以下の説明では、5.1節で説明した(1)中間事業者型の事業モデルにおけるケースで説明する。

以下で説明するサービスは、電力センサを使った住宅の消費電力見える化サービスとする。システム構成は図5-4のようになる。消費電力をグラフとして表示する端末はスマートフォンとして、スマートフォンのブラウザに表示するものとする。スマートフォンは携帯電話網、または住宅内のWiFi AP経由で接続される。また、電力センサは、ECHONET Liteデバイスであり、ECHONET Liteプロトコルにより規定される情報の取得が可能である。

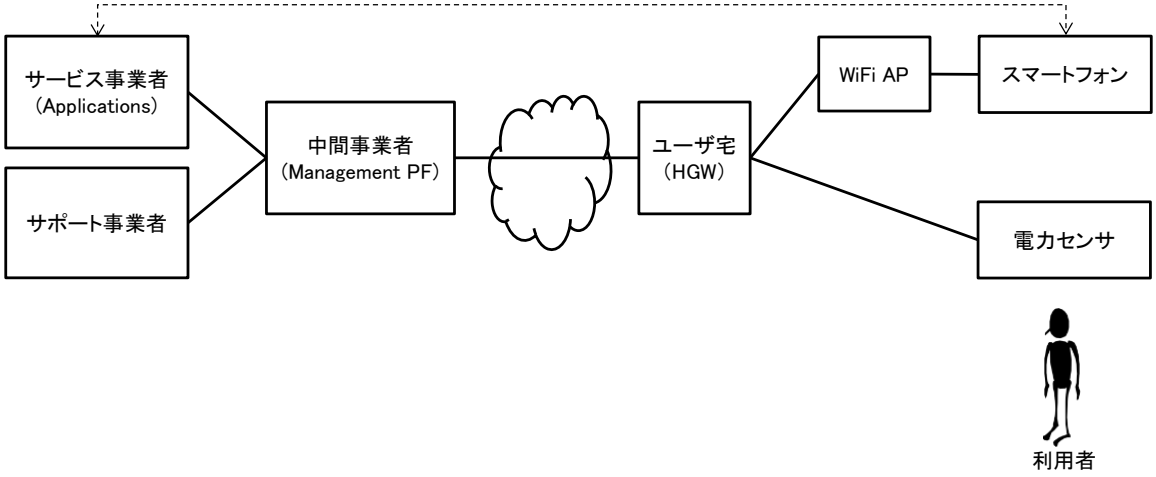

図5-4　見える化サービスのシステム構成

以下では、このシステム構成に基づいて説明する。ただし、既にネットワーク機器の設置・設定は完了し、HNサービスに必要なデバイスの設置するところから始めるものとする。

(1)サービス/デバイス登録

エンドユーザが見える化サービスを利用するには、サービス利用の登録と必要な端末の登録が必要となる。図5-5にはこの流れを示した。

見える化アプリケーションはWebアプリケーションとして提供されるため、ここではスマートフォンのWebブラウザを通じてサービス登録を行う。サービス登録を行う際には、ユーザ宅の情報（ユーザID、電力センサの情報等）をアプリケーションに登録する。アプリケーションは、リソース管理にサービス情報を登録する。一方、電力センサはサービス登録後、エンドユーザ宅のHNに接続するとHGWは端末を検出して、HGWのデバイス管理がManagement PFのリソース管理に端末情報を通知する。この際に、あらかじめアプリケーションから登録されていたユーザIDと端末情報を比較することにより、合致していれば正式に端末が登録される。

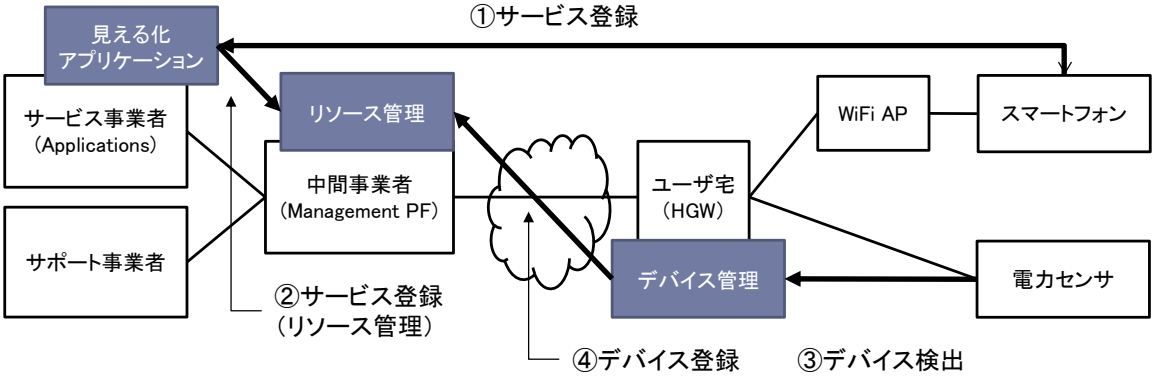

図5-5　サービス登録・デバイス登録

(2)デバイス自動設定

端末が登録されると、HGWを通じて電力センサに必要な設定情報が通知され、自動的に設定される（図5-6）。図5-6には記載していないが、電力センサで設定が終了すると、HGWを通じてリソース管理に電力センサの設定完了が通知される。この通知を受けて、リソース管理は見える化アプリケーションに対してデバイス登録の完了を通知する。この通知をもって、このユーザ宅での消費電力見える化サービスが利用可能となる。

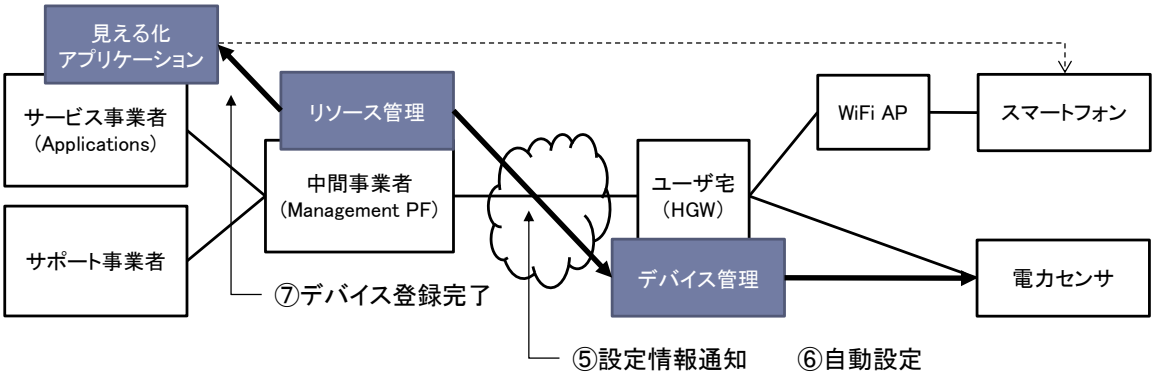

図5-6　デバイス自動設定

(3)サービス利用開始

図5-7は、サービスが正常に動作しているときのデータの流れである。サービスを利用するには、スマートフォンのWebブラウザから見える化アプリケーションにアクセスする。アプリケーションは、定期的に取集する電力センサのデータ（消費電力）をスマートフォンに通知するか、見える化画面を作成してブラウザに表示する。一方で、電力センサからのデータは、HGWがECHONET Liteプロトコルを利用して定期的に取得するか、定期的に通知されるようにしておき、HGWは収集したデータをManagement PFに通知する。アプリケーションはManagement PFからデータの通知を受けて、アプリケーションで必要なデータを蓄積する。この蓄積されたデータが、スマートフォンからの要求により通知されるわけである。

なお、サービスが正常に動作中にも、HGWやManagement PFでは3章で述べた機能を使用して、ユーザ宅のHNにおけるリソース情報を定期的に収集する。

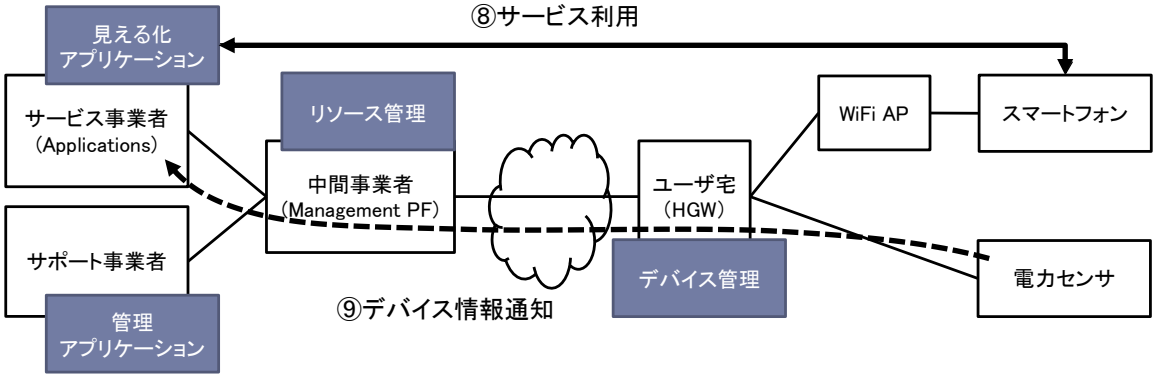

図5-7　サービス利用開始

(4)エンドユーザからの障害通知

図5-8は、エンドユーザ宅で何らかの障害が発生し、電話やメール等の手段によってコールセンタに通知されるケースを示す。ユーザからコールセンタに通知されると、コールセンタの保守員は管理アプリケーションを通じて、Management PFに蓄積されるユーザ宅のリソース情報を参照する。ここでは、見える化アプリケーションで使用するデバイス（電力センサ）の状態を照会する。Management PFは最新のデバイス情報を取得済みであればその情報を表示するが、取得されていない場合にはHGWのデバイス管理に問い合わせを行い取得する。

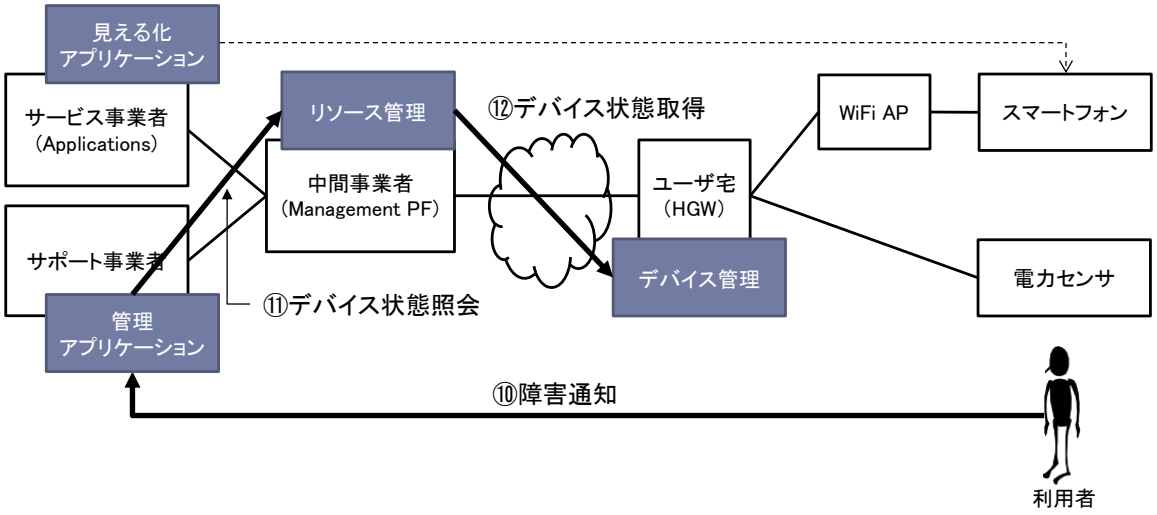

図5-8　エンドユーザからの障害通知

(6)障害からの復旧

図5-9は、取得したデバイス情報に基づき、保守員は原因を分析する。ここでは、端末の設定情報に問題があったとする。この場合には、コールセンタからユーザに対して復旧に際して、端末の設定情報の変更が必要であることを通知し、ユーザの了解をもらったうえで、サポート事業者は以下の操作を行う。サポート事業者は、管理アプリケーションを通じて、リソース管理に対してこのユーザ宅のデバイス情報の設定を変更する。Management PFのリソース管理では、ユーザ宅のHGWにおけるデバイス管理に対して端末の設定情報を通知すると、デバイス管理に登録された設定情報に基づいて、デバイス（電力センサ）の設定情報が自動設定され、障害が解消する。

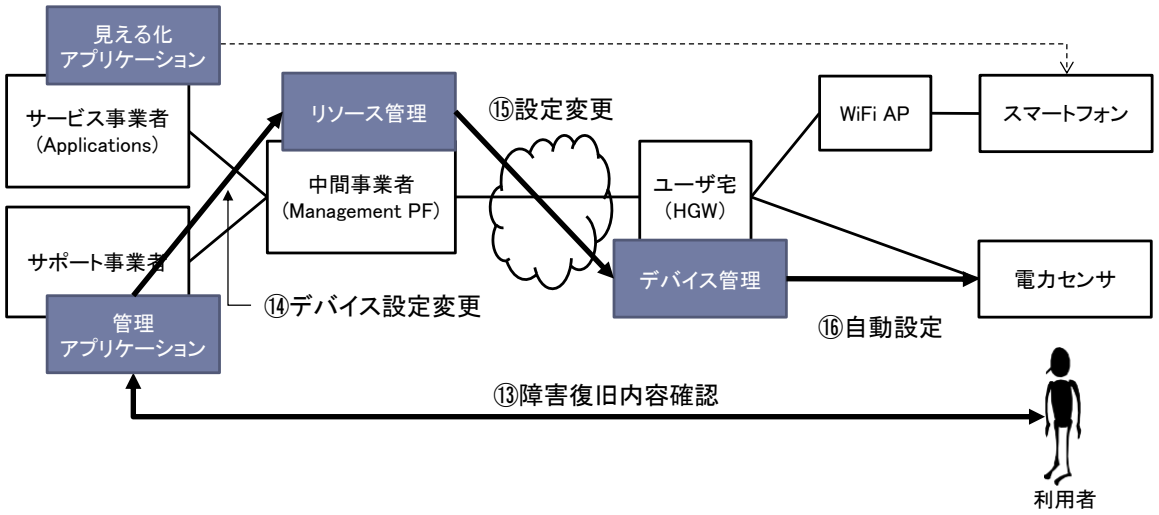
見える化
アプリケーション
サービス事業者
(Applications)
サポート事業者
管理
アプリケーション
リソース管理
中間事業者
(Management PF)
⑮設定変更
⑭デバイス設定変更
ユーザ宅
(HGW)
デバイス管理
WiFi AP
スマートフォン
電力センサ
⑯自動設定
⑬障害復旧内容確認
利用者

図5-9　障害復旧

第6章　まとめ

本技術レポートでは、HNサービスの普及に伴い、大きな課題となることが予想されるカスタマサポート機能について述べた。HNに接続される端末は今後増加が期待され、また様々な通信方式やプロトコルが混在するために、複雑な構成になることが考えられる。それに伴い有効なカスタマサポートを実現するためには、HN内の端末やネットワークの状況を個別に把握し、HGW、管理PFとネットワークの上流で統合するアーキテクチャを明確化し、ここで述べたように各々に要求される機能が必要になる。このアーキテクチャでは、カスタマサポート機能がユーザ宅で発生している問題を正確に把握し、必要に応じて設定を変更したり、試験トラフィックを流すなどしてユーザに代わって障害からの復旧プロセスを実行できるメカニズムも必要になろう。また、HNの設置される家には専門的な知識をもつ管理者が不在であり、障害が発生したときにその状況をうまく表現できず、カスタマサポート機能の支援を十分に受けられないことが予想される。今後は、ここで定義された端末に具備すべき機能をもとに、ITリテラシーの高くない一般ユーザを想定し、個々のカスタマサポート機能の有効性を実証するためのケーススタディの実施と、複数の端末提供者にその有効性をどのようにPRし、その機能の実装を促進するかが次の課題である。

参照文献

[ATM OAM] ITU-T Recommendation I.610 (1999), B-ISDN operation and maintenance principles and functions

[ISO/IEC 30100] ISO/IEC 30100-1 (2013), Information technology – Home network resource management – Part 1: Requirements

[IEC 62608] IEC 62608-1 (2013), Multimedia home network configuration – Basic reference model – Part 1: System model

[ITU-T G.9980] ITU-T Recommendation G.9980 (2012), Remote management of customer premises equipment over broadband networks – customer premises equipment WAN management protocol

[BBF TR-069] BBF TR-069 (2011), CPE WAN Management Protocol

[BBF TR-181] BBF TR-181 (2012), Device Data Model for TR-069

[DLNA] IEC 62481-1 (2006)、DLNA Home networked device interoperability guidelines Part 1: Architecture and Protocols

[DHCP] IETF RFC2131 (1997), Dynamic Host Configuration Protocol

[DHCPv6] IETF RFC3315 (2003), Dynamic Host Configuration Protocol for IPv6

[Ethernet OAM] ITU-T Recommendation Y.1731 (2013), OAM functions and mechanisms for Ethernet based networks

[ICMP] IETF RFC792 (1981), Internet Control Message Protocol, IETF RFC4443 (2006), Internet Control Message Protocol for the Internet Protocol Version 6 (IPv6) Specification

[LLDP] IEEE 802.1ab (2005), Station and Media Access Control Connectivity Discovery

[MIB] IETF RFC1213 (1991), Management Information Base for Network Management of TCP/IP-based internets: MIB-II

[PPPoA] IETF RFC2364 (1998), PPP Over AAL5

[PPPoE] IETF RFC2516 (1999), A Method for Transmitting PPP Over Ethernet

[SNMP] IETF RFC1157 (1990), A Simple Network Management Protocol

[RA] IETF RFC4861 (2007), Neighbor Discovery for IP version 6

[Telnet] IETF RFC854 (1983), Telnet Protocol Specification

[TTC HTIP] TTC JJ-300.00 v1.1 (2011), HN接続構成特定プロトコル

[TTC TR-1046] TTC TR-1046 (2013), ホームネットワークサービスを実現するサービスプラットフォーム

[TTC TR-H.QoS(Sup11)] TTC TR-H.QoS(Sup11) (2009)、クラス型ホームネットワークQoS技術の分析

[KNX] ISO/IEC 14543-3-x (2006), OSI-based network communication protocol for intelligent buildings

[ZigBee SEP2.0] ZigBee Alliance, Smart Energy Profile 2.0 Application Protocol.

[ECHONET Lite] ECHONET Consortium, ECHONET Lite Specification Version 1.01.

[UPnP] ISO/IEC 29341-x (2011), Information technology – UPnP Device Architecture

[UPnP DM] UPnP DM (2012), UPnP Device Management: 2