

TR-1086

HTIP 評価ツール  
及び構築ガイドライン

〔 HTIP evaluation tools and implementation guideline 〕

第 1.0 版

2021 年 3 月 2 日制定

一般社団法人  
情報通信技術委員会

THE 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

.....	1
<参考> .....	4
1. はじめに .....	5
1.1 背景 .....	5
1.2 ユースケース .....	6
1.3 HTIP エージェント、マネージャ .....	9
1.4 ネットワーク機器での動作.....	9
1.5 非 Ethernet/非 IP への対応.....	10
2. HTIP 関連 OSS .....	11
2.1 lwhtip .....	11
2.2 node_htip .....	12
2.3 Wireshark プラグイン : LuaHTIP .....	13
2.4 FreeHTIP .....	13
2.5 HTIP 評価環境の構築.....	14
3. 実用的な機器への実装例.....	15
3.1 HTIP 対応デバイス.....	15
3.2 HTIP 対応ネットワーク機器.....	16

## <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	2021年3月2日	制定

### 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 : IoTエリアネットワーク専門委員会 (SWG3603)

### 5. 本技術レポートの制作体制

本レポートは、スマートIoT推進フォーラム技術・標準化分科会(会長:丹康雄[JAIST])において原案を作成し、その後TTC IoTエリアネットワーク専門委員会(委員長:西川嘉樹[NTT])での審議を経てTTC技術レポートとして公開するものである。

技術・標準化分科会における検討については、IoTエリアネットワークOAMタスクフォース(リーダー:松倉隆一[富士通研究所])にて作業を行った。

# 1 はじめに

本技術レポートでは、IoTエリアネットワークのトポロジ及び障害を検出するためのガイドラインについて解説する。

## 1.1 背景

JJ-300.00(HTIP: Home network Topology Identifying Protocol)は、ホームネットワークに接続される機器のネットワーク構成(トポロジ)を検出するプロトコルとして開発された。その後、ITU-T G.9973として国際規格となっている。通信事業者等がホームネットワークに設置される機器の遠隔からメンテナンスする際に、ブロードバンドルータとその先に接続されるネットワーク機器、そしてそのネットワークに接続されるPCやスマートフォンなどのネットワーク構成情報が必要である。JJ-300.00は、ホームネットワーク上のネットワーク機器やPC等のデバイスに搭載されることが想定される。その後、ホームネットワークではセンサや家電などの様々な機器がつながるようになり、ホームネットワーク内で発生する障害を検出し、原因を切り分けることが難しくなっている。この状況はIoTの普及に伴い、ホームネットワーク以外でも課題となってきた。そこで、接続されるIoTデバイスやネットワーク機器からメンテナンスに必要な情報を提供してもらい、あらゆる機器からの情報を総合して問題となる個所を見出すことが提案された(TR-1053/57)。この提案に基づき、JJ-300.00が第2版、第3版と改版され、対応可能なIoTデバイスの種類が大幅に増えた。現在では、JJ-300.00(第3版)に対応したOSSが開発、公開されており、この規格が利用しやすくなっている。

本技術レポートは、JJ-300.00に関心があり、評価環境を検討されている方を対象としている。以下では、JJ-300.00の概要、開発されたOSS、実用的な機器への適用方法等について解説する。OSSは、Raspberry Piのようなハードウェアで動作するため、比較的簡単に試すことができる。

JJ-300.00(第1版)により実現される機能イメージを図1に示す。この図では、接続される機器情報(製造メーカ、製品名、型番)、隣接する機器の情報(ネットワーク機器については、ポート番号も)が通知されるため、これらの情報を統合することによってエリアネットワークの全体構成を得ることができる。JJ-300.00の第2版では、TR-1053およびTR-1057の提案に基づいて、障害検出に必要な情報を通知できるように拡張している。障害検出に必要な情報としては、例えば、無線通信する機器に関しては無線の受信信号の強度などがあげられる。

また、第1版では、Layer2の機能(LLDP)を利用しているため、ネットワークをEthernetに限定して実現している。第2版、第3版では、非Ethernet、非IPネットワークに拡張し、IoTで利用されるネットワークのほとんどをカバーできるようになっている。

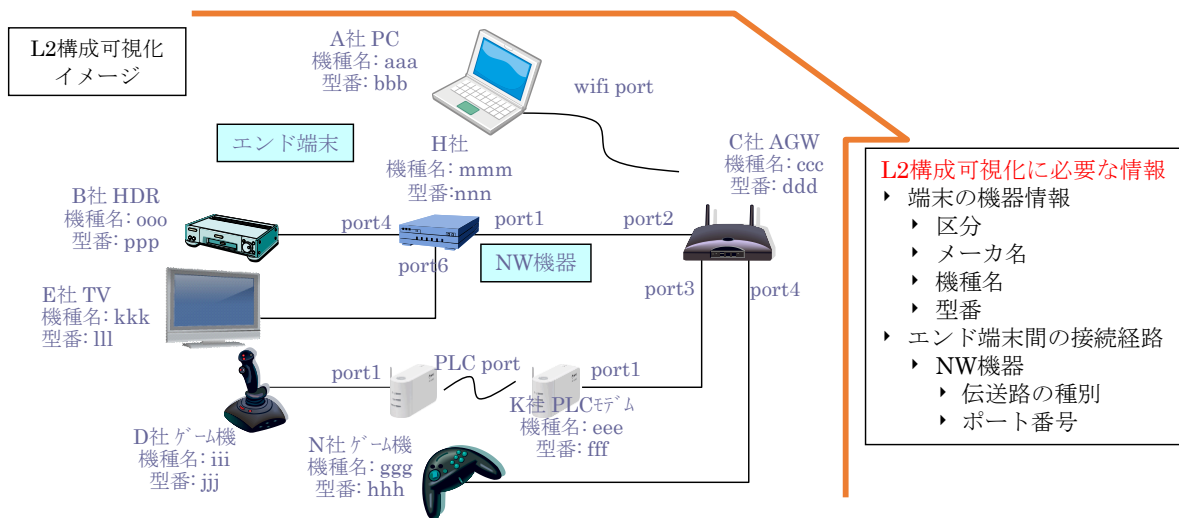


図1. HTIPの概要

## 1.2 ユースケース

### 1.2.1 アセットマネジメント

住宅、ビル、工場、街などに設置される IoT デバイスやネットワーク機器の状態をリモートから監視する。スマートホームやスマートビルディングのようにサービスとして接続する機器を管理するが、アセットマネジメントでは、販売したメーカーや量販店が、販売した装置を直接管理するケースが該当する。販売者が保守サービスとして、交換が必要な消耗品・部品の状況を確認したり、定期点検に必要な運用情報を収集したりする。

サービス事業者が設置したデバイス、ネットワーク機器に関しても同様のサービスを提供する。

図 2 にアセットマネジメントの例を示す。点線に囲まれた部分がユーザのローカルネットワークである。このユースケースでは、ユーザのネットワークに接続されるネットワーク機器（ブロードバンドルータ、無線ルータ）とその先に環境を計測するセンサ（温度、照度など）を接続する。これらのセンサ情報をクラウドで収集し、ブラウザ等で参照したり、これらのセンサ情報をもとにして、ユーザにリコmendしたり、空調機等の制御を行ったりする。このサービスが継続的に利用できるようにするために、ネットワーク機器やその先に接続されるセンサが安定して動作していることを確認するために、それぞれに HTIP エージェントを搭載し、ローカルネットワーク内に接続される HTIP マネージャでこれらの情報を集約する。HTIP エージェントでは、データの通信品質、装置自身の状態について HTIP エージェントを通じて発信を行い、これらの情報を分析することで機器の異常や障害を検出することを目的とする。アセット管理者は、各ユーザの HTIP マネージャから情報を得ることで、ユーザに代わってユーザの機器のマネジメントを行うことができる。

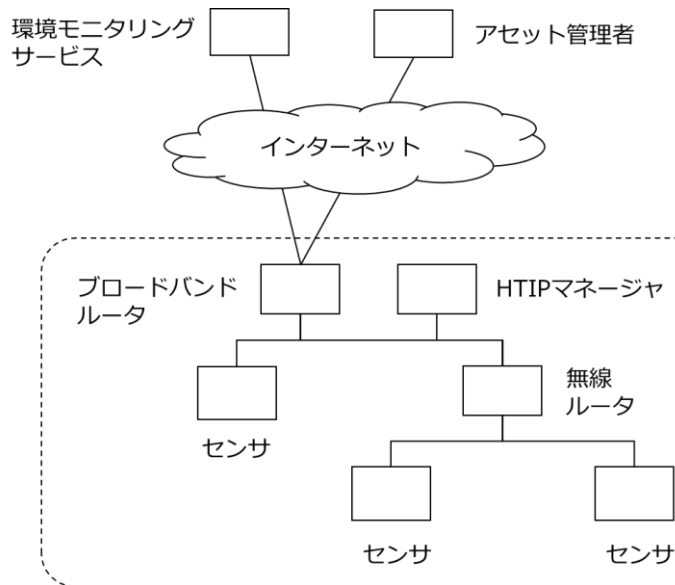


図 2. アセットマネジメントの例

### 1.2.2 スマートホーム

スマートホームのサービス提供者が、設置したコントローラやスマートロック等の機器が正常に動作していることを監視し、機器やネットワークのトラブルによりサービスが停止することを防ぐ。

図 3 にスマートホームの例を示す。点線に囲まれた部分がユーザのローカルネットワークである。このユースケースでは、ユーザのネットワークに接続されるネットワーク機器（ブロードバンドルータ、無線ルータ）とその先に家電（エアコン、照明等）とセンサを接続する。スマートホームのアプリケーションは、ローカルネットワークに接続されるホームコントローラが、センサ情報に合わせてエアコンや照明を最適に制御する。または、センサ情報をクラウドにあるスマートホームサービスに通知して、クラウドでアプリケーションを動かすことも可能である。

一方で、このサービスが継続的に利用できるようにするために、ネットワーク機器やその先に接続される家電やセンサが安定して動作していることを確認するために、それぞれに HTIP エージェントを搭載し、ローカルネットワーク内に接続される HTIP マネージャでこれらの情報を集約する。HTIP エージェントでは、データの通信品質、装置自身の状態について HTIP エージェントを通じて発信を行い、これらの情報を分析することで機器の異常や障害を検出することを目的とする。設置機器のモニタリングサービスは、スマートホームサービスと独立するケースもあるが、同じ事業者が提供するケースを図3に示した。

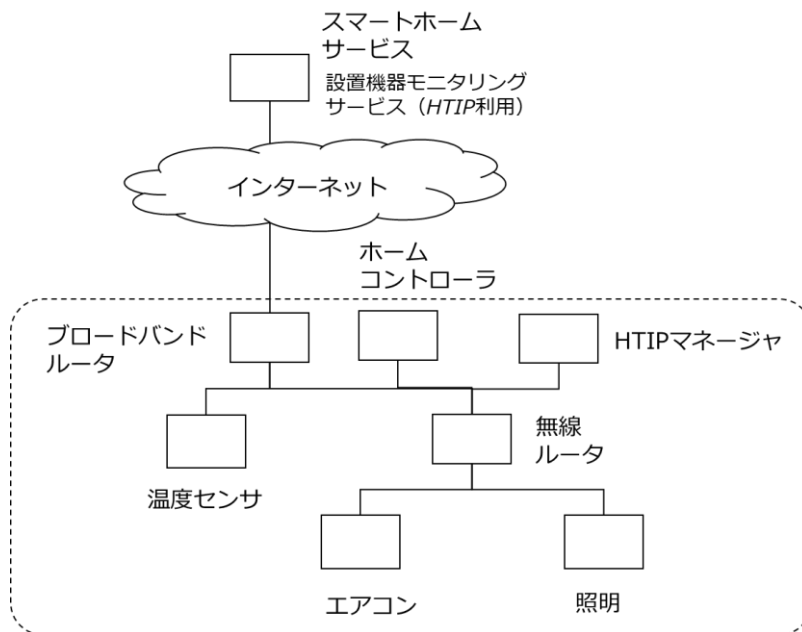


図3. スマートホームの例

### 1.2.3 スマートファクトリ

生産現場に設置される製造装置や運搬装置の稼働情報、保守情報等を収集する。生産停止に至る可能性のある装置やネットワークのトラブルを回避したり、生産効率を改善する情報として利用する。現場に設置される装置は、長期間にわたり利用されることが多く、古い規格のインタフェースの装置が多い。そのため、生産装置に振動センサや音センサを接続して、異常振動や異常音を検出する仕組みをスマートファクトリのサービスの一部として実現することもある。

図4にスマートファクトリの例を示す。点線に囲まれた部分がユーザのローカルネットワークである。このユースケースでは、ユーザのネットワークに接続されるネットワーク機器（ブロードバンドルータ）とその先に工場の建屋の空調設備やセンサと、PLC (Programmable Logic Controller) を経由して工場の生産設備等が接続される。特に PLC 以下のネットワークを OT (Operational Technology) ネットワークとして IT ネットワークとは別に扱われることが多い。工場の生産設備が接続されるネットワークのトラブルは、生産停止などの大きなトラブルにつながりやすいため、ネットワークが常に使用可能になっていることが重要である。最近では、OT ネットワークにおいても無線が利用されるようになり、無線伝搬に大きな影響を及ぼす金属設備が多い工場では、ネットワークの通信状態を監視することが求められている。PLC や生産設備については、Ethernet を L2 で利用する EthnerCAT など、様々な通信媒体が使われる。HTIP エージェントをどこまで適用できるかについては、今後検討が必要である。

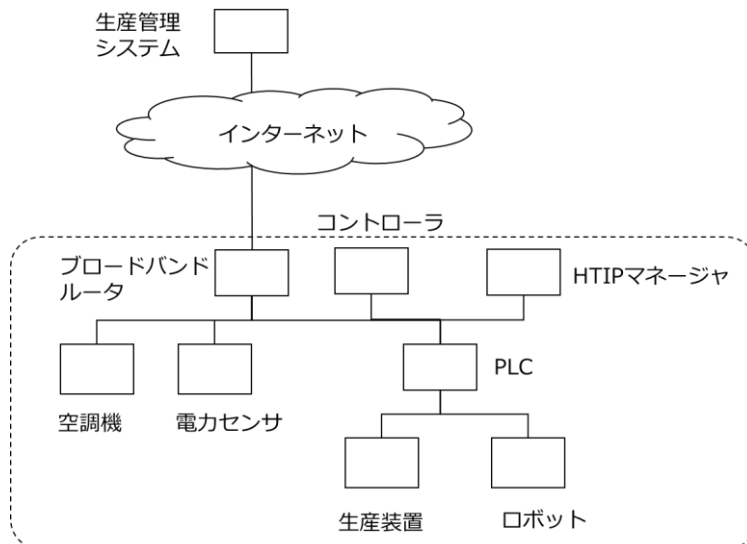


図4. スマートファクトリの例

#### 1.2.4 運用支援(インストール、監視)

これまで、サービス利用時における障害検出のユースケースを説明してきた。一方で、IoT サービスが拡大するにつれて、装置の設置やネットワーク接続といったインストール時のトラブルへの対応も必要である。IoT 機器は、機能やインタフェースの種類が多様であるが、インストール作業者がその全てに精通しているとは限らない。また、最近では、ユーザ自身がインストールを行い、オンラインでアクティベートするケースも増えており、インストール中のトラブルを遠隔から監視し、遠隔から修正することが重要になってくる。

図5はICT機器の導入支援サービスの例である。点線内は工事を行うホームネットワークである。例えば、図右下にある温度センサを無線アクセスポイント経由で接続する際には、接続した温度センサの情報がICT機器設置サービスに通知される。現地での作業者は、設置した装置が十分な電波の受信強度を確保できているかどうか、接続すべきネットワークに正しく接続されているかなど、クラウドサービスで知ることができる。もし無線の信号強度が低い場合には、障害物等を確認の上、センサやアクセスポイントを移動して、問題を解決することができる。このようにJJ-300.00は装置設置後の装置やネットワークの監視だけでなく、設置時の動作確認にも利用することができる。

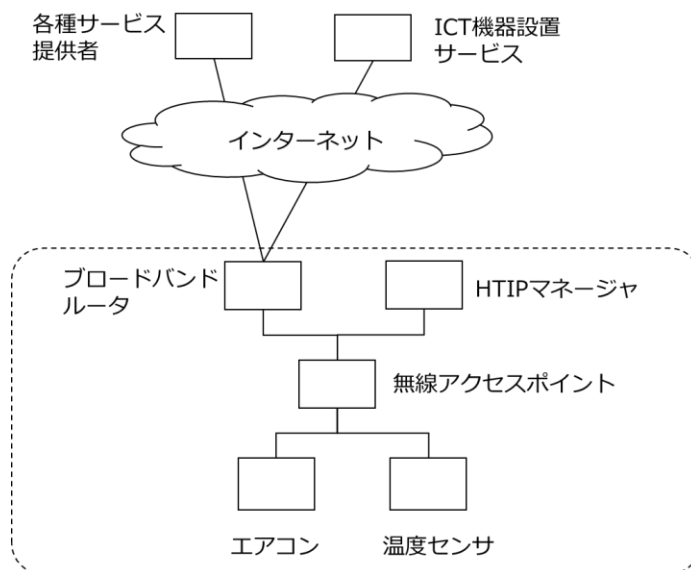


図5. ICT機器導入支援サービスの例



### 1.3 HTIPエージェント、マネージャ

HTIP はエージェントとマネージャからなる。エージェントは、IoT デバイスやネットワーク機器、サーバなどに搭載される。エージェントは、その機器内の情報を取得し、LLDP でその情報を発信することを基本としている。マネージャは、これらの機器の情報を集約することによって、隣接する機器の情報、機器内部の情報を統合することによって、接続される機器全体のネットワーク構成と、障害の発生有無とその原因について分析できる。

図 6 は HTIP 端末の基本的な構成を示した。HTIP 端末は、HTIP エンド端末と HTIP ネットワーク (NW) 端末からなる。HTIP エンド端末は、デバイスやサーバなどの端末である。HTIP ネットワーク端末は、HTIP エンド端末や他の HTIP ネットワーク端末を接続する役目を持つ。したがって、ネットワークに接続される機器は、エンド端末かネットワーク端末に属する。HTIP 端末には HTIP エージェントが動作する。HTIP エージェントには、L2 で動作するものと L3 で動作するものがあり、L2 エージェントは LLDP を利用して通信を行う。L3 エージェントは UPnP 等のプロトコルを利用する。HTIP マネージャは HTIP エージェントが発信する HTIP メッセージを集集し、収集した情報からネットワークのトポロジを推定する。また、HTIP エージェントの情報には、端末の内部状態や通信状態の情報も含まれるため、ネットワークトポロジとともに、端末及びそれらをつなぐネットワークの状況を可視化することができる。

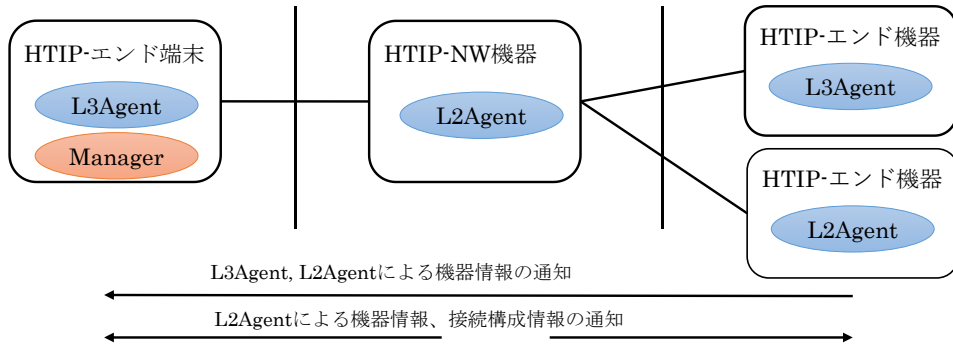


図 6. HTIP マネージャ、エージェントの構成

### 1.4 ネットワーク機器での動作

HTIP エージェントから送信される情報は、ネットワーク機器で中継され、HTIP マネージャに通知される。全ての機器が Ethernet で接続される場合には、ネットワーク機器で受信した HTIP エージェントのメッセージを中継する。デバイスやネットワーク機器が Ethernet に対応していない場合には、HTIP エージェントで取得した情報を、デバイスやネットワーク機器が対応する通信方式によって通知を行い、Ethernet に対応するネットワーク機器において LLDP に変換して送信する。

図 7 は、HTIP による IoT エリアネットワークにおける運用管理機能を実現するサービスアーキテクチャである。図の中央にあるゲートウェイ (GW) は、エリアネットワークとインターネットの境界にあり、2 つのネットワークをつなぐ役割を果たす。1.3 で述べた HTIP マネージャとエージェントは、このゲートウェイの右側のネットワークの構成を示す。HTIP は、L2 (LLDP) で通信するため、1.2 のユースケースで説明したようなクラウドからの運用管理に対応するには、ゲートウェイを通じて Web API のようなインターネットに対応したインターフェースが必要となる。管理 PF はこうしたゲートウェイからの情報を集約するプラットフォームであり、ここに集約されたデータを分

析・監視することによって、クラウドからの保守を実現することができる。

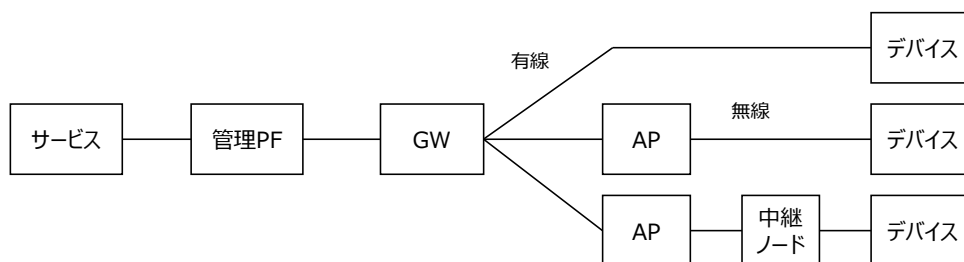


図7. サービスアーキテクチャ

### 1.5 非Ethernet/非IPへの対応

今回の評価ツールは、IP ベースで、Ethernet 及び Wi-Fi に対応した機器が対象である。しかし、IoT で利用される装置のインタフェースとしては、RS-485 のようなシリアルインタフェースや、Bluetooth のような無線が利用されており、こうした装置が同じ JJ-300.00 で管理できることは重要である。これらの機器においては、障害検知に対処するためにエラーコードや内部状態を出力するインタフェースを備えることが多いため、非 IP/非 Ethernet のインタフェースについては、IP/Ethernet インタフェースを持つ中継器を経て、中継器に搭載される HTIP エージェントから再送信される仕組みが必要となる。

詳細については、TTC TR-1061 及び TR-1073 を参照されたい。

## 2. HTIP関連OSS

HTIPを利用するには、JJ-300.00に基づいてエージェントとマネージャを開発する必要がある。また、エージェントとマネージャの動作を確認するために、ネットワーク上を流れるパケットを解析するツールがあると便利である。この章では、OSSとして提供されているソフトウェアについて説明する。

### 2.1 lwhtip

lwhtipはエンド端末とNW機器向けのHTIP L2エージェントの実装である。本エージェントは定期的にHTIP情報をネットワークに送信する。NW機器向けの実装ではOSが管理するFDB(Forwarding DataBase)を利用することで接続構成情報も含んだHTIP情報をネットワークに送信する。NW機器として動作させる際には一般的なブリッジとして動作するように先に設定を行う。

lwhtipはC言語で実装され主にlinux上で動作する。OSS (MIT License)としてgithub (<https://github.com/Tan-Lab/lwhtip>)で公開されている。

インストールと実行に必要なパッケージ(debianの場合)

- build-essential, autoconf, libtool, bridge-utils

インストール手順は以下の通りである。

- autoreconf -fi
- ./configure
- make
- make install

エンド端末エージェントの実行手順は以下の通りである。

- インストール済みの場合
  - l2agent
- 未インストールの場合
  - src/bin/l2agent

NW機器エージェント 実行手順は以下の通りである。

- ブリッジインタフェースの作成
  - 例) eth0 と eth1 のブリッジインタフェース br0 を作成する場合
    - ◇ brctl addbr br0
    - ◇ brctl addif br0 eth0
    - ◇ brctl addif br0 eth1
- インストール済みの場合
  - l2switch -i br0
- 未インストールの場合

➤ `src/bin/l2switch -i br0`

wireshark/tcpdump等のツールを用いることで定期的に宛先MACアドレスがff:ff:ff:ff:ff:ffでフレームタイプ0x88ccのフレームが送信されていることを確認することができる。

## 2.2 node\_http

node\_httpはトポロジの可視化を行うHTIPマネージャの実装である。ネットワーク上に流れるHTIPメッセージを受信しJSON形式で保持する。また保持している情報はHTTPを用いてWebブラウザに転送される。Webブラウザ上で接続構成情報等の解析を行うことで、ネットワークトポロジーを生成し可視化を行う。

node\_httpはLinuxとmacOS上で動作する。JavaScriptで実装されておりNode.jsを用いて実行される。OSS (MIT License)としてgithub ([https://github.com/Tan-Lab/node\\_http](https://github.com/Tan-Lab/node_http))で公開されている。

インストールに必要なパッケージ(debianの場合)

- nodejs, npm, net-tools, libpcap-dev

インストール手順は以下の通りである。

- `npm install`
- `node-gyp configure build`

実行手順は以下の通りである。

- `npm start`

可視化方法は以下の通りである

- Web ブラウザ (firefox 等) で HTIP マネージャが動作しているホストのポート 3000 番にアクセスする。  
➤ 例) <http://localhost:3000/>

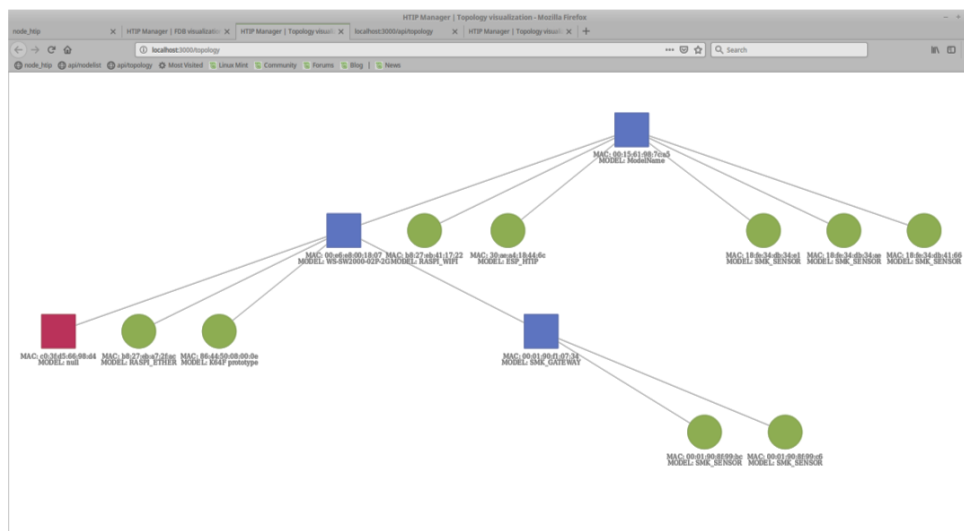


図 8. HTIP マネージャ (node http) のトポロジー表示

### 2.3 Wiresharkプラグイン : LuaHTIP

LuaHTIPはwireshark向けのHTIPプラグインである。このプラグインを利用することによって、ユーザに分かりやすくHTIPフレームの情報を表示できる。これにHTIPフレームの構造を簡単に確認ができる。

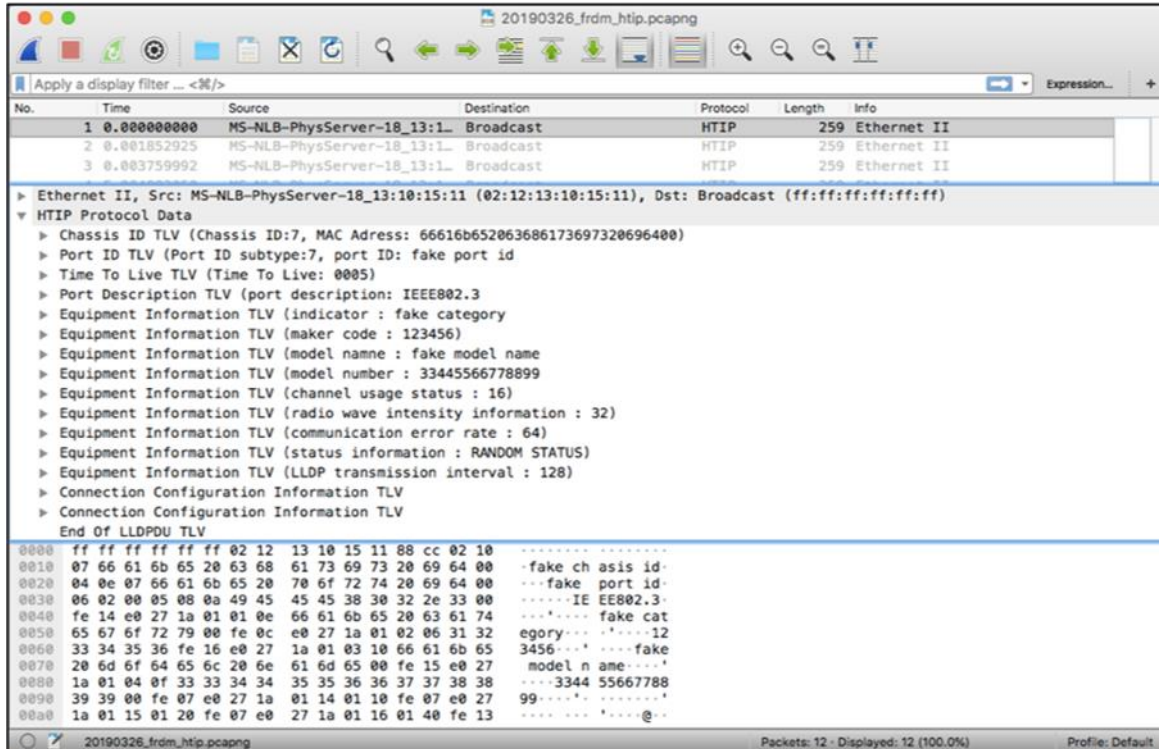


図 9. LuaHTIP プラグインを利用した Wireshark の表示例

このプラグインはLua言語で記述されている。wiresharkのプラグインフォルダーに本プラグインをコピーし、本プラグインを実行するようにinit.luaファイルを編集することでインストールを行う。インストール方法の詳細はWiresharkのドキュメント([https://www.wireshark.org/docs/wsug\\_html/#ChPluginFolders](https://www.wireshark.org/docs/wsug_html/#ChPluginFolders))に記述されている。

LuaHTIPはOSS(MIT License)としてgithub(<https://github.com/Tan-Lab/LuaHTIP>)で公開されている。

### 2.4 FreeHTIP

FreeHTIPは組み込み機器向けのHTIP L2 エージェント (エンド端末) の実装である。ライブラリとして組み立てられていて、HTIPフレームの作成と解析機能を提供している。

ライブラリとして提供されているため、その機能を組み込み機器に取り入れたい時は、既存のプロジェクトに追加しソースコードを編集する必要がある。HTIPフレームの作成例としてl2agent.cを参照し、組み込むプロジェクトに合わせて修正してください。

現在までにESP32とFRDM-K64Fを使用する組み込み機器での動作実績がある。これらの実装ではFreeRTOSというRTOSにlwipというTCP/IPプロトコルスタックと組み合わせて実行しているが、FreeHTIPはFreeRTOSとlwipに依存していないため、他のRTOSやTCP/IPプロトコルスタックとの組み合わせでも動作するはずである。

FreeHTIPは、OSS (BSD-2 clause)としてgithub (<https://github.com/s-marios/FreeHTIP>)で公開されている。

## 2.5 HTIP評価環境の構築

本章で説明したHTIP関連OSSを利用して構築可能なHTIP評価環境の例を図10に示す。

この例では、4ポートのHUBに1台のHTIPマネージャと3台のHTIPエンド端末が接続されている。4ポートHUBは、4個のUSBポートにUSBネットワークアダプタを接続したRaspberry Pi3を利用し、Linuxの機能を利用してHUBを実現している。具体的には、4個のEthernetをブリッジ接続している。HTIPエンド端末は、Raspberry Pi3とFRDM-K64Fを利用して実現している。Raspberry Pi3にはLinux、FRDM-K64FにはFreeRTOSがインストールされており、HTIPエージェントはそれぞれlwhtipとFreeHTIPをインストールしている。HTIPマネージャはLinux PCで動作しており、node\_htipを利用してしている。図の左に表示されるトポロジ表示では、1台のHUB（青）と3台のHTIPエージェント（緑）、HTIPマネージャ（赤）が表示されている。また、このネットワーク上に流れるHTIPメッセージについては、WiresharkにLuaHTIPをプラグインとして登録することによって表示することができる。

この評価環境は、入手しやすいハードウェアで構成しており、2章で解説したOSSをインストールすることで簡単に構築することが可能である。

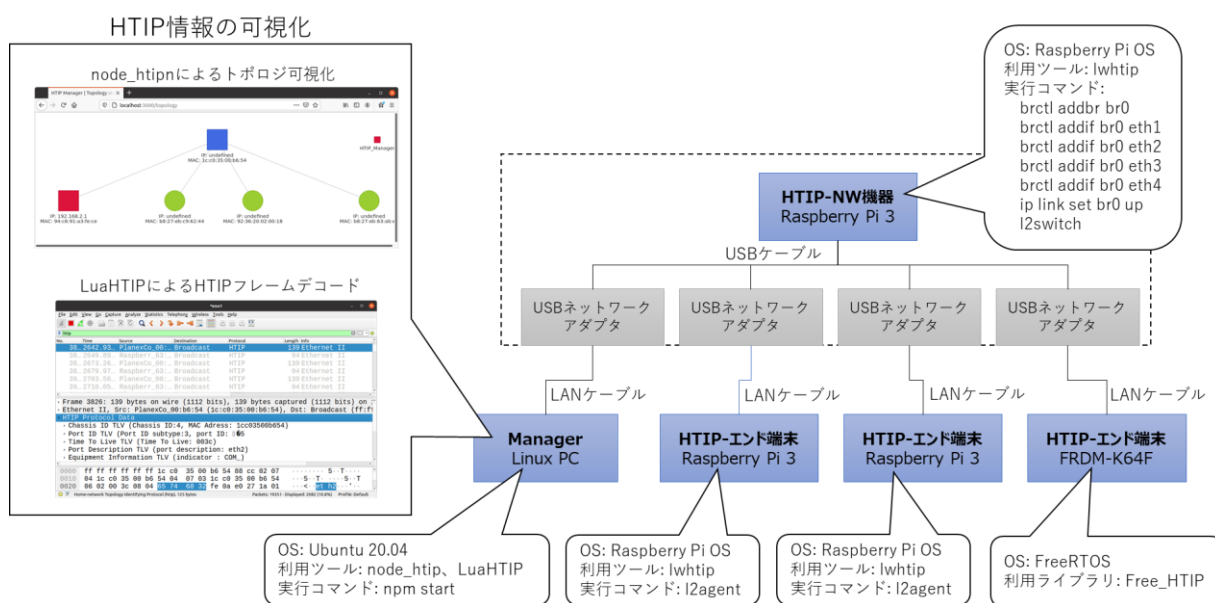


図10. OSSを利用したHTIP評価システム例

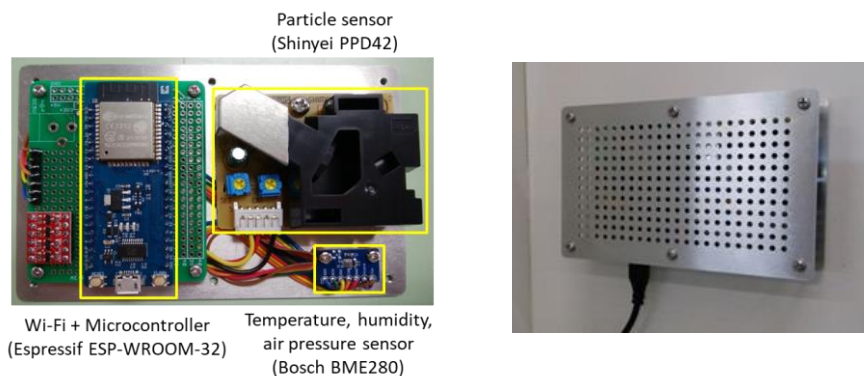
### 3. 実用的な機器への実装例

HTIPを利用して、実際のフィールドに適用したデバイスやネットワーク機器の事例を紹介する。

#### 3.1 HTIP対応デバイス

工場における環境情報（温湿度、ダスト）を測定するセンサの事例を図11に示す。

MPUを搭載したWi-Fiモジュール（ESP-WROOM-32）に、Bosch社製の温湿度・気圧センサとShinyei社製のダストセンサを接続したセンサ装置を開発し、工場内に設置して環境情報を収集する。工場においては、有線ネットワークを新たに施設することは難しいうえ、製造ラインのレイアウトが頻繁に変更されるために無線を利用することとした。しかし、無線ネットワークは電波の障害物等の影響により通信トラブルが多く、その状況を把握するためにもHTIPを活用している。



(左：搭載部品、右：外観)

図11. 工場に設置したセンサ装置

Wi-Fi通信モジュール上のMPUで動作するソフトウェア構成を図12に示す。ソフトウェアは、搭載されるセンサの初期化、制御を行う機能（図12左側）とHTIPで運用情報を通信する機能（図12右側）、W3Cで規定されるWeb of Thingsで通信する機能（図12中央）からなる。Web of Thingsによる通信機能は、センサ装置の外部からのインターフェースとなっており、センサ情報の取得やWi-Fi通信モジュールの設定や情報取得等のやり取りは、Web of Thingsで規定されるWeb APIによって実行される。一方で、デバイス情報やデータ通信時の無線信号強度（RSSI）、その他、デバイスの運用に関する情報（電池残量、通信エラー率など）は、JJ-300.00で規定されるHTIPエージェントがデバイス制御・運用管理機能から情報を取得して、Wi-Fiドライバを通じて通信される。

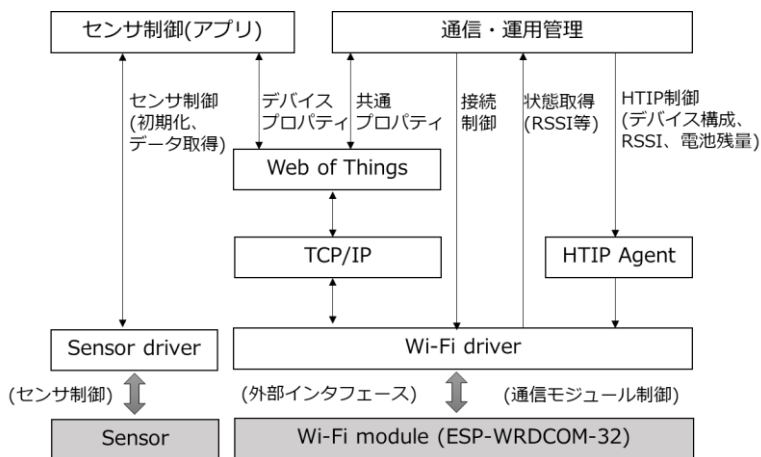


図12. センサ装置のソフトウェア構成



実際の工場では、40台以上のセンサ装置を設置し、2年以上利用されている。Wi-Fi APにはhostapdをRaspberry Piにインストールし、図12のHTIPエージェントを搭載したものを10台設置している。これらのAPを通じて取得したセンサ装置の情報を工場内のサーバ（HTIPマネージャ）で収集している。

図13は、1台のセンサ装置から取得されたセンサ情報及びHTIP情報の時間経過を表示したものである。左から気圧、無線通信強度（RSSI）、温度を示しており、1分ごとに取得されたデータが表示されている。無線信号強度が2回に渡り劣化している様子が見られるが、これはセンサ装置とAPとの間にある通路を運搬車が通過したために生じたものである。このように無線は知らない間に通信状況が変化することがあり、劣化した状態が継続するとトラブルとして露見することになる。このようにHTIPを利用して通信状況を記録することで、トラブルを事前に把握できる可能性がある。

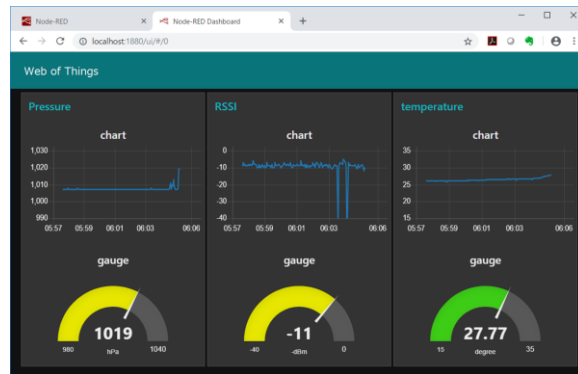


図13. センサ装置から得られる情報

### 3.2 HTIP対応ネットワーク機器

既存製品をベースにHTIPエージェントを組み込んだ事例と、ユースケースを説明する。

#### 3.2.1 L2SWとWi-Fi AP

##### (1) L2 Switch (WS-SW2000-02P-2G)

図14にL2SWの外観と、図15にその仕様を示す。

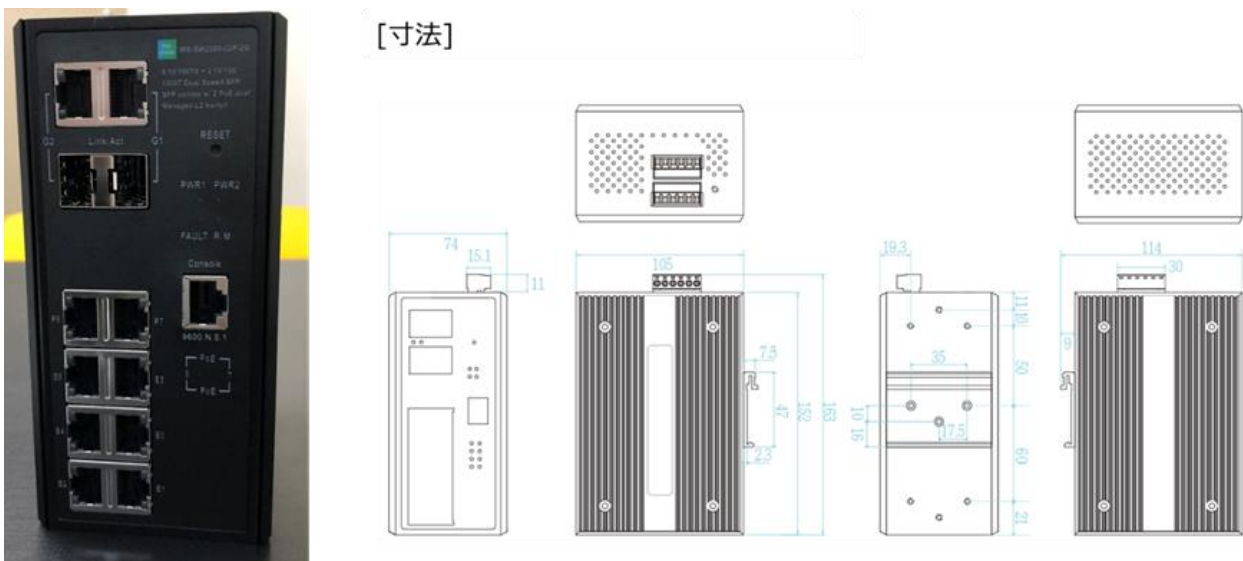


図14. HTIP対応L2SW外観





インターフェース	
LANポート数	10
SFPスロット数	2
microSDスロット	-
PoE	
PoE給電可能ポート	8
最大給電能力（1ポートあたり）	12W 48V
最大給電能力（装置全体）	30W @54V(at)
性能	
スイッチング容量	7.4Gbit/s
VLAN	
VLAN	○
IPマルチキャスト	
Layer2	○
管理/設定	
コンソールポート接続	○
ブラウザ接続	○
ハードウェア	
動作条件	-20°C～75°C
外形寸法	72mm (W) x 105mm (D) x 152mm (H)

図15. HTIP対応L2SW仕様

(2) Wi-Fi AP (WS-AP2000-01P-1G)

図16にWi-Fi APの外観と、図17にその仕様について説明する。

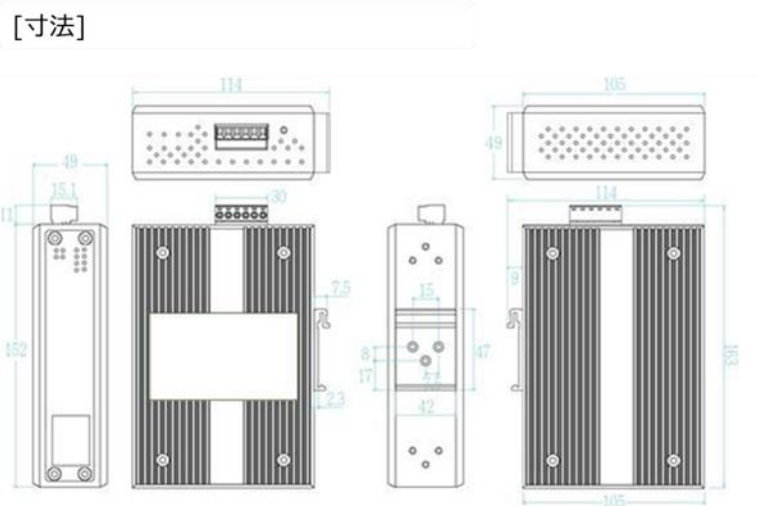


図16. HTIP対応AP仕様



無線LAN部	
無線LAN規格	IEEE802.11ac 最大300Mbps
	IEEE802.11n 最大300Mbps
	IEEE802.11g 最大54Mbps
	IEEE802.11b 最大11Mbps
周波数帯域	2.4GHz、5GHz
セキュリティ規格	WEP、WPA (PSK,EAP対応)、WPA2 (PSK、EAP対応)
有線部	
LANインターフェイス有線LAN(HUB)ポート数	8
端子	RJ-45(コンソールポート)
ハードウェア	
動作環境条件	-20~70°C
外形寸法	74.3mm (W) x 109.2mm (D) x 153.6mm (H)

図17. HTIP対応AP仕様

(3) ファームウェアの特徴 (共通アーキテクチャ)

HTIP運用エージェントとして、L2 Switch、Wi-Fi APそれぞれにHTIP(ITU-T G.9973)を実装し、IoTエリアネットワーク内の機器の運用管理を目的としたHTIPのオプション項目を実装した。これらのネットワーク機器では、接続デバイス数、アクティブノード数、CPU使用率、メモリ使用率、LLDPDU送信間隔と、Wi-Fi APではこれらに加えて、電波強度や無線品質 (パケット再送など) の実装を行った。HTIPに関する機能は、共通の関数として表現することにより、L2SwitchおよびWi-Fi APで共通のアーキテクチャとなっている。そのため、様々な機器へのHTIP搭載が容易な構造になっている。図18、図19には、L2 SwitchとWi-Fi APのLLDPDUフレーム構成を示す。

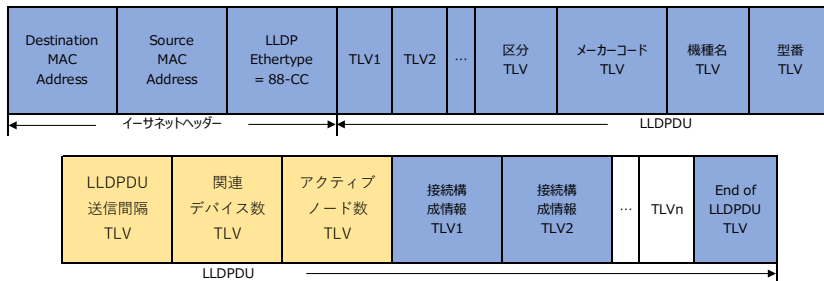


図18. 実装したL2 SwitchのHTIP LLDPDUフレームの構成

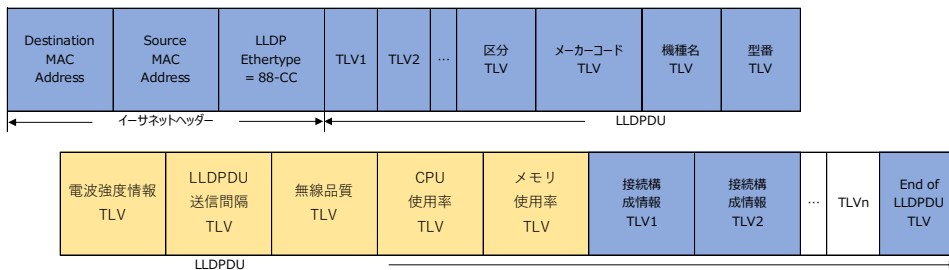


図19. 実装したWi-Fi APのHTIP LLDPDUフレームの構成

#### (4) NW機器の耐熱性

IoTの様々なフィールド、例えば農業や様々な産業用途に利用可能とするためには、ホームやオフィスに比較して厳しい温度環境(-20℃~70℃)での動作が求められる。ここで紹介する機器に関しては恒温槽を使用し、-20℃と70℃の環境で、20時間連続してパケットの送受信を繰り返す環境試験を実施している。

#### 3.2.2 ユースケース（駐車場管理システム）

Ethernet対応の監視カメラ、LoRaWAN対応の駐車状況取得用のセンサ、またBLE用のセンサなどを活用する、通信方式によらない拡張性の高い駐車場システムを実現した。複数の通信方式が混在するシステムで問題になるのは、それぞれのデバイスの保守運用管理である。そこで、それぞれの機器にHTIPプロトコルを組み込むことで、HTIPマネージャにより、各センサは、通信方式によらず、可視化され、初期不良や通信不良、設定不良などを早期に発見することが可能となる。また、HTIP情報をサーバ側に保存することにより、デバイスの設置場所や設置環境による、センサの経年劣化などに伴う交換の必要時期を把握することが可能となるため、センサに対する保守運用管理も実現可能となる。さらに、駐車場空き情報を表示するシステムなどと組み合わせることにより、保守運用をしやすいIoTシステムを実現する。

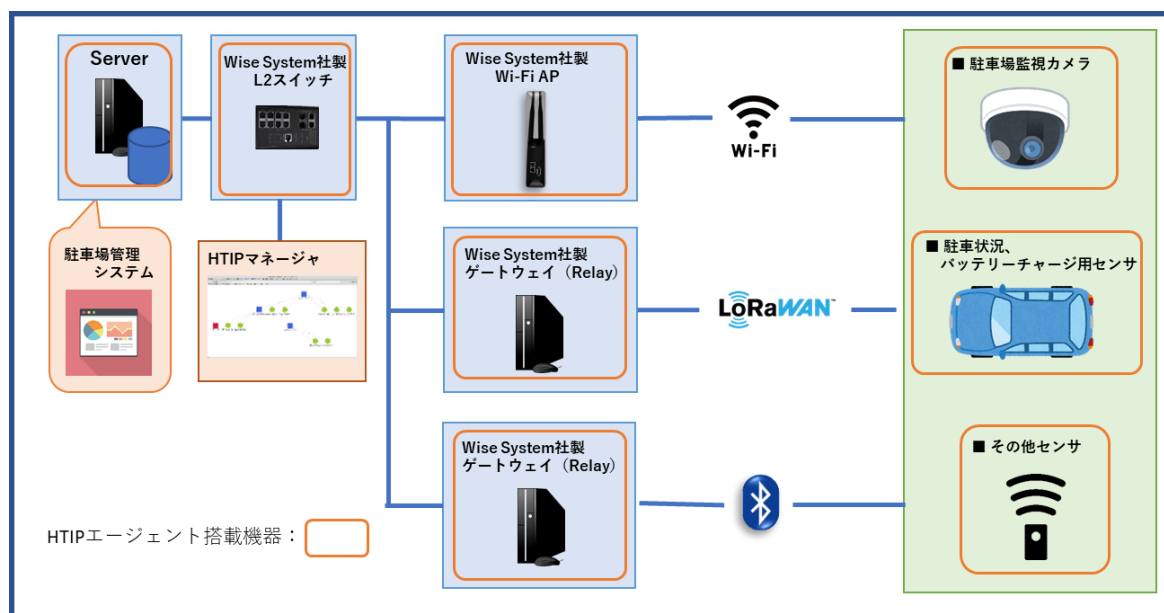


図20. 駐車場管理システムの構成