米国における IoT 基盤の動向調査

JETRO/IPA New York

1　はじめに

IoT に対する注目は最近ますます高まってきており、企業、大学、政府などはさまざまな形で IoT にかかわろうと動き出している。そうした中、調査会社 Gartner 社が 2016 年 3 月に興味深いプレスリリースを出した。そのプレスリリースとは「2017 年の IoT テクノロジ・トレンドのトップ 10[1]」というものである。プレスリリースの内容そのものが興味深いのはもちろんのこと、それ以上に興味深いのは同社が IoT にフォーカスした技術トレンドを調査し発表しているという点である。プレスリリースの冒頭は、「これからの 2 年間を通じてすべての企業・組織にとって重要性が増してくるであろうモノのインターネット (IoT) テクノロジのトップ 10 を発表しました」という書き出しで始まっており、これを見ると IoT は今後重要なのかどうかという議論はすでに不要なものとなっており、今やどのようなテクノロジが今後の IoT 業界をリードするのかということを考える時期に来ていることがわかる。

そのような状況の中で、IoT にかかわろうと動いている企業はいずれも、この新しい市場の中でいち早く優位なポジションをとるために、積極的な取り組みを行っている。そのような企業の一社である GE 社は、これまでの重厚長大な企業というイメージを一新し、産業界向けの IoT ビジネスを柔軟に展開することで、業界で主導的な役割を果たそうと動いている。以下の図表 1 は、自社の工場にオバマ大統領を招いて共に見学する GE CEO のジェフリー・イメルトである。

図表 1：GE を見学するオバマ大統領と GE CEO のジェフリー・イメルト

出典：Forbes[2]

[1] https://www.gartner.co.jp/press/html/pr20160311-01.html
[2] http://www.forbes.com/sites/adrianbridgwater/2015/11/04/electric-dreams-ge-widens-industrial-iot-vision/ -1e4c37c75a86

この GE 社が IoT 業界で果たそうとしている役割のひとつに、IIC（Industrial Internet Consortium）という IoT 基盤を提供する業界コンソーシアムでの主導的な立場がある。今後、産業界向けの IoT が発展していく際に必ず必要となってくる標準化活動を推進しながら、同時に実装のために欠かせないテストベッドを提供するという取り組みにより、IIC は IoT 業界において重要なポジショニングをとろうと動いており、それを主導しているのが GE 社である。

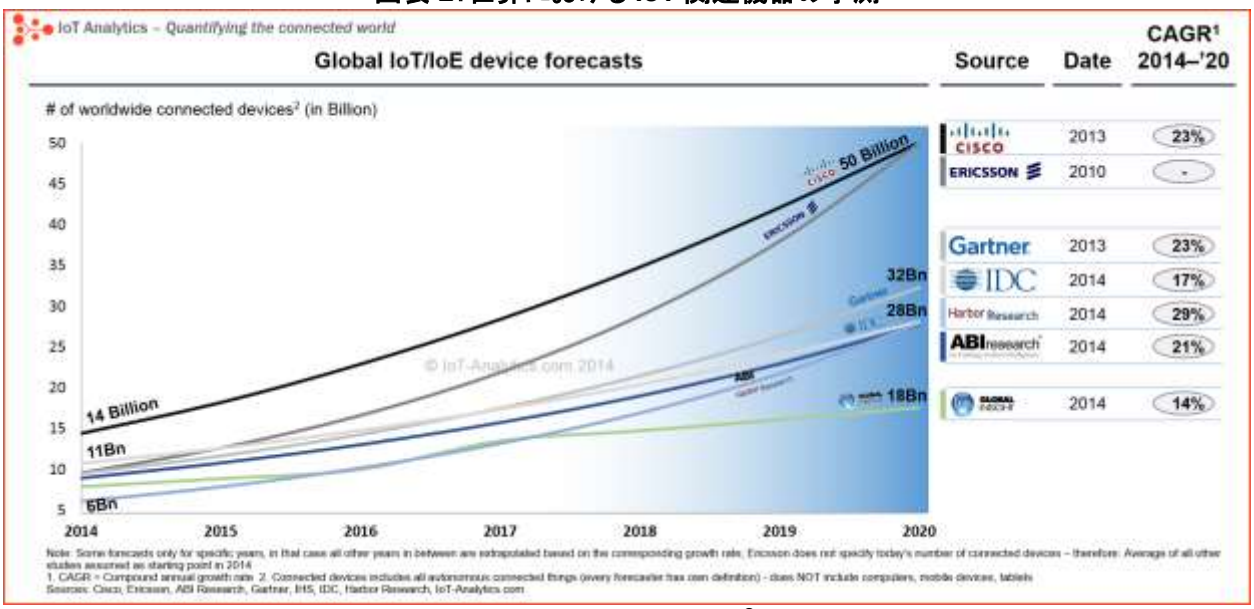
本レポートでは以下、IoT 市場の最新の動向を簡単に紹介した上で、GE 社が主導する業界コンソーシアム IIC のような IoT の発展に欠かせない IoT 基盤を策定する業界団体の動向を紹介しながら、IoT の技術進化や今後のビジネス展開を整理する。なお、本レポートで使う「IoT 基盤」という言葉は、IoT 機器をつなぐ時に利用出来るソフトウェアプラットフォームという意味合いで使っている。言い換えれば、ソフトウェアの構造とアプリケーションインタフェース(API)が規定されているようなものを想定して「IoT 基盤」という言葉を利用している。

2　IoT 市場の最新動向

（1） IoT 市場に関する予測

この数年で、さまざまな企業が今後の IoT 市場の成長見込みや動向に関する調査結果を発表している。当然ながら、どの調査結果も市場が拡大するというものとなっており、IoT 市場の成長を疑う声はない。以下の図表 2 は、世界における IoT 関連機器、つまり通信ネットワークに接続されるあらゆる機器の数の推移にフォーカスし、調査会社各社の予測をまとめたグラフとなっている。

図表 2:世界における IoT 関連機器の予測



出典:IoT Analytics[3]

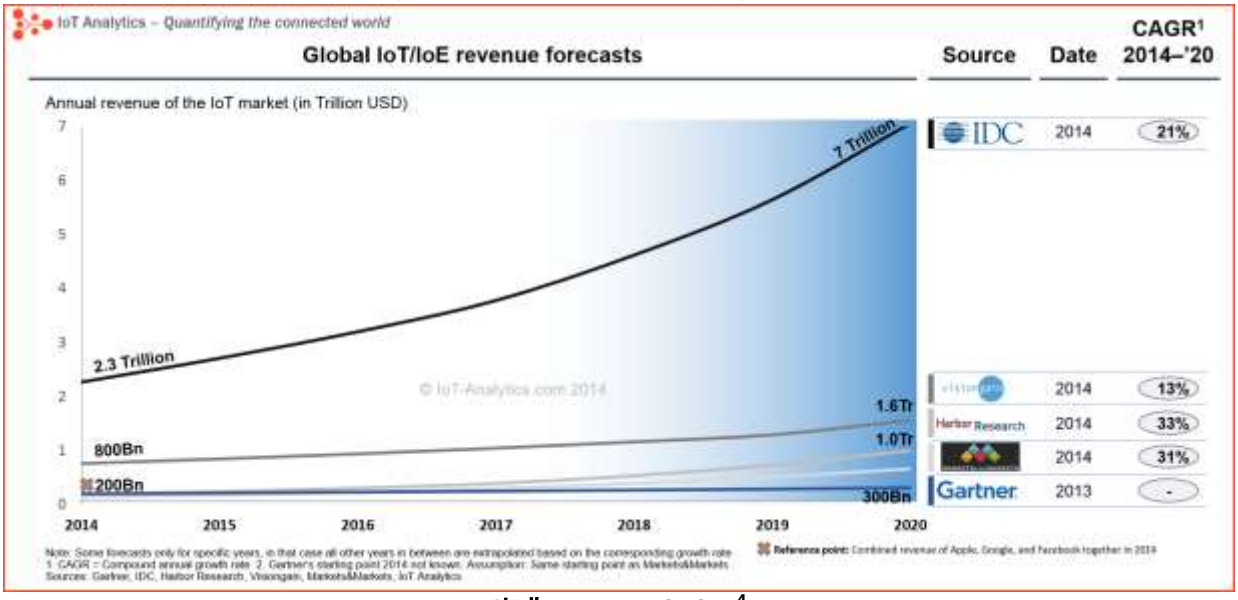
このグラフによると、2014 年時点では世界において 60 億台（Harbor Research 社の予測）～140 億台（Cisco 社の予測）の IoT 機器がネットワークにつながっているとされている。なお、この場合の機器（Things）にはパソコンやスマートフォン、タブレットなどの端末は含まれていない。その後の 2020 年までの推移を見ても、各社とも予測値は大きく異なっているものの、いずれも増加する傾向で考えている点で共通している。最も控えめな予測をしている IHS Global Insight 社でも 180 億台となっており、最も積極的な予測をしている Cisco 社と Ericsson 社については 2020 年には 500 億台の機器がネットワークに接続されていると予測している。その中間的な予測をしているのが Gartner 社の 320 億台や IDC 社の 280 億台である。

なお、この予測値の差は各社の予測手法や根拠とするデータの違いから生まれたものに過ぎないが、最も積極的な予測をしている Cisco 社と Ericsson 社については、注意が必要である。これは、両社が他の調査会社と違って IoT 関連の事業に直接的に関与しており、市場を盛りたてる立場にあるためである。市場が成長することによる直接的なメリットが両社にあるという点を考えると、Gartner 社や IDC 社といった純粋な調査会社による中間期な予測が現実的であると想像できる。いずれにせよ、それでも市場は大きく成長すると見られる。

[3] http://iot-analytics.com/iot-market-forecasts-overview/

次の図表 3 は、世界における IoT 市場の売上規模を金額で表したグラフである。これもさまざまな企業による予測値を一枚にまとめたグラフとなっている。ただし、IoT 機器の推移数にフォーカスした上記の図表 2 と異なり、この売上規模予測には Cisco 社や Ericsson 社といった IoT 事業に直接関与する一般企業のものは含まれておらず、すべて純粋な調査会社による予測値をまとめたものとなっている。

図表 3:世界における IoT 市場規模の予測



出典:IoT Analytics[4]

上記からもわかるように、市場規模の予測値は IDC 社だけ突出して大きくなっている。例えば、2014 年時点の値は、Markets&Markets が 2,000 億ドルであるのに対して、IDC は 2 兆 3,000 億ドルであると試算している。2020 年の予測値を見ても、最も控えめな予測が Gartner 社の 3,000 億ドルであるのに対し、最も強気な予測をしている IDC 社は 7 兆ドルにのぼるとしている。なお、この市場規模の予測値の差について、出典元は特に説明をしていないが、「IoT」の定義が各社の間で異なる状況にあることが影響している可能性が高い。例えば、IoT 市場は機器、アプリケーション、ソリューション、通信サービス、サポートなどあらゆる事業コンポーネントで構成されるが、このどれをもって「IoT 市場」と定義しているのか、その他の経済効果を含むのか、などについて各社で違いがあると考えられる。

とはいえ、今後 IoT 市場が成長していくことは間違いないものの、2020 年に IDC 社が予想するような 7 兆ドル規模にまで発展するかというと、疑わしい面は拭えない。特に、世界レベルであってもこれだけの大きな経済効果を本当に生み出すのかという点から、例えば 2014 年の日本の GDP である約 4.6 兆ドル[5]をみると、2020 年の予測値がいかに大きな数値であるかが伺える。こうした点を考えれば、2020 年の予測値としては、その中間にある 1.6 兆ドル(Visiongain の予測)や 1 兆ドル(Harbor Research の予測)という数値が現実的ではないかと考えられる。いずれにしても、市場規模も IoT 機器の数と同様に、2020 年に向けて成長基調にあることは間違いないと言える。

[4] http://iot-analytics.com/iot-market-forecasts-overview/
[5] https://www.google.co.jp/publicdata/explore?ds=d5bncppjof8f9_&met_y=ny_gdp_mktp_cd&idim=country:JPN:CHN:MEX&hl=ja&dl=ja

（2） ビジネスとしての IoT の活用分野

上記の調査会社による予測データから、IoT 市場は今後数年にわたって機器数、売上ともに大きく成長する有望な分野であることが確認できた。では、実際にどのような分野が IoT の技術進化や普及による影響を受けるのであろうか。それらをまとめたものが以下の図表 4 である。

この図表 4 では、消費者向け（to C）とビジネス向け（to B）に分類した上で、それぞれ IoT の活用が想定される分野と具体的に対象となるビジネス分野を整理している。これを見るとわかるように、IoT はあらゆる分野に浸透すると考えられていることから、IoT が関係しない分野を探す方が難しいほどの状況にある。つまり、IoT は今後ビジネスのあらゆる側面に影響を与えていくことになると言える。

図表 4：IoT の活用分野

顧客タイプ	分野	対象となるビジネス分野
消費者向け（to C）	家	・ホームオートメーション ・家の環境改善 ・エネルギー効率化
	ライフスタイル	・ウェアラブル ・エンターテイメント＆音楽 ・家族 ・レジャー ・ペット ・おもちゃ ・ドローン
	ヘルスケア（医療）	・フィットネス ・モニタリング ・データ計測 ・診断
	移動	・コネクテッド・カー ・e バイク
ビジネス向け（to B）	小売	・小売店 ・コンビニエンスストア
	医療（ヘルスケア）	・モニタリング ・データ計測 ・診断 ・手術 ・患者ケア
	エネルギー	・送配電 ・化石燃料 ・原子力 ・代替エネルギー源
	移動	・航空宇宙・空港 ・船舶 ・列車・駅 ・自動車 ・交通
	都市	・インフラ ・水・廃水 ・空調 ・照明

		・セキュリティ ・安全
	製造	・鉱山 ・石油・ガス ・生産 ・サプライチェーン
	公共サービス	・学校 ・大学 ・政府 ・銀行 ・保険 ・行政 ・一般向けサービス
	その他	・環境 ・軍事 ・農業

出典：各種情報を基に作成[6]

次に、IoT のビジネスへの影響を具体的に数値で示したデータを紹介する。以下の図表 5 は、大手コンサルティング会社 McKinsey 社の資料をもとに、IoT の導入により価値が生まれるとされる分野とその市場規模を整理したものである。

McKinsey 社が IoT 導入により価値が生まれる分野としてあげたのは、左側に示した 9 分野（①工場：オペレーションマネジメント、予知保全、②都市：公共の安全、健康、交通量コントロール、資産管理、③人：病気の監視や管理、健康増進、④小売：セルフレジ、レイアウト最適化、スマート CRM[7]、⑤屋外：ロジスティックの経路決定、自動運転、ナビ、⑥作業場：オペレーション管理、機器保守、安全衛生、⑦乗り物：状態基準保守、保険料削減、⑧家庭：エネルギー管理、安心・安全、家事自動、⑨その他：組織再編、作業者監視、トレーニングへの AR 活用[8]）となっている。右側に示されているのは、各分野の 2025 年における世界レベルの市場規模であり、最少額と最大額の幅で予想されている。

9 分野のうち 2025 年に最も市場規模が大きくなると考えられているのが工場向けの IoT であり、1.2 兆ドル～3.7 兆ドルの市場規模になると予想されている。これに続いて規模が大きくなると考えられているのが都市向けの IoT であり、その規模は 9,000 億ドル～1.7 兆ドルと予測されている。9 分野全ての市場規模を合算すると、2025 年における世界レベルの IoT 市場の規模は 4 兆ドル～11 兆ドルにのぼるという予想になっている。

[6] http://iot-analytics.com/iot-market-segments-analysis/
https://www.cbinsights.com/blog/iot-market-map-and-company-list/
[7] スマート CRM とは、IoT をもって CRM（Customer Relationship Management：顧客関係管理）をデータドリブンに行いスマート化するというコンセプト。
[8] トレーニングへの AR 活用とは、AR グラスなどを装着することで現実環境を拡張させながら社員のトレーニング体験を充実させるというコンセプト。

図表 5：IoT 導入により価値が生まれる分野

【工場】オペレーションマネジメント、予知保全

【都市】公共の安全、健康、交通量コントロール、資産管理

【人】病気の監視や管理、健康増進

【小売】セルフレジ、レイアウト最適化、スマート CRM

【屋外】ロジスティックの経路決定、自動運転、ナビ

【作業場】オペレーション管理、機器保守、安全衛生

【乗り物】状態基準保守、保険料削減

【家庭】エネルギー管理、安心・安全、家事自動化

【その他】組織再編、作業者監視、トレーニングへの AR 活用

出典：McKinsey[9]

[9] http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

3　米国における IoT 基盤の動向

（1） IoT 基盤が目指す役割

IoT に関連する技術が進化する中、IoT ビジネスに参入をする企業は後を絶たず、今後とも IoT ビジネスを展開する企業は増加の一途を辿ると考えられている。そうした中、業界で懸念されているのは、IoT サービスやデバイス間の相互運用性（interoperability）である。相互運用性とは、異なるハードウェアやソフトウェアであっても、お互いに問題なくデータのやり取りなどの連携ができることを意味している。

IoT ビジネスでは、あらゆるモノやサービスを相互に接続し、データをやり取りしたりサービスを連携させたりすることで、新たな価値を生み出すことが想定されている。ただし、相互に接続するモノやサービスが、すべて同じ企業のものであることは限らない。仮に同じメーカーの IoT 製品やサービスであっても、場合によっては製品やサービスが 5 年、10 年と比較的長期間の利用を想定しているケースもあり、相互接続の対象となる製品やサービスを開発・提供する企業が異なるだけでなく、それらが市場に投入されたタイミングが異なるような状況が容易に考えられる。

例えば、ある A 社の HEMS（Home Energy Management System）製品を導入したユーザが、HEMS 製品に別の B 社のサーモスタットと C 社の家電を接続して一括で管理しようとする場合を考えてみる。この場合、仮に A 社の HEMS 製品が自社製品以外を制御できる仕様になっていなければ、このユーザは A 社の HEMS 製品を導入した意味がなくなってしまう。また、この HEMS 製品を 5 年間使い続けた後に同じ A 社の最新のサーモスタットを購入した場合、もし HEMS 製品が最新のサーモスタットに対応する仕様になっていないと、同じ A 社の製品であってもユーザは HEMS 製品を買い換えるなどし、改めて家庭内のホームコントロールシステム環境を設定し直さなければならなくなってしまう。

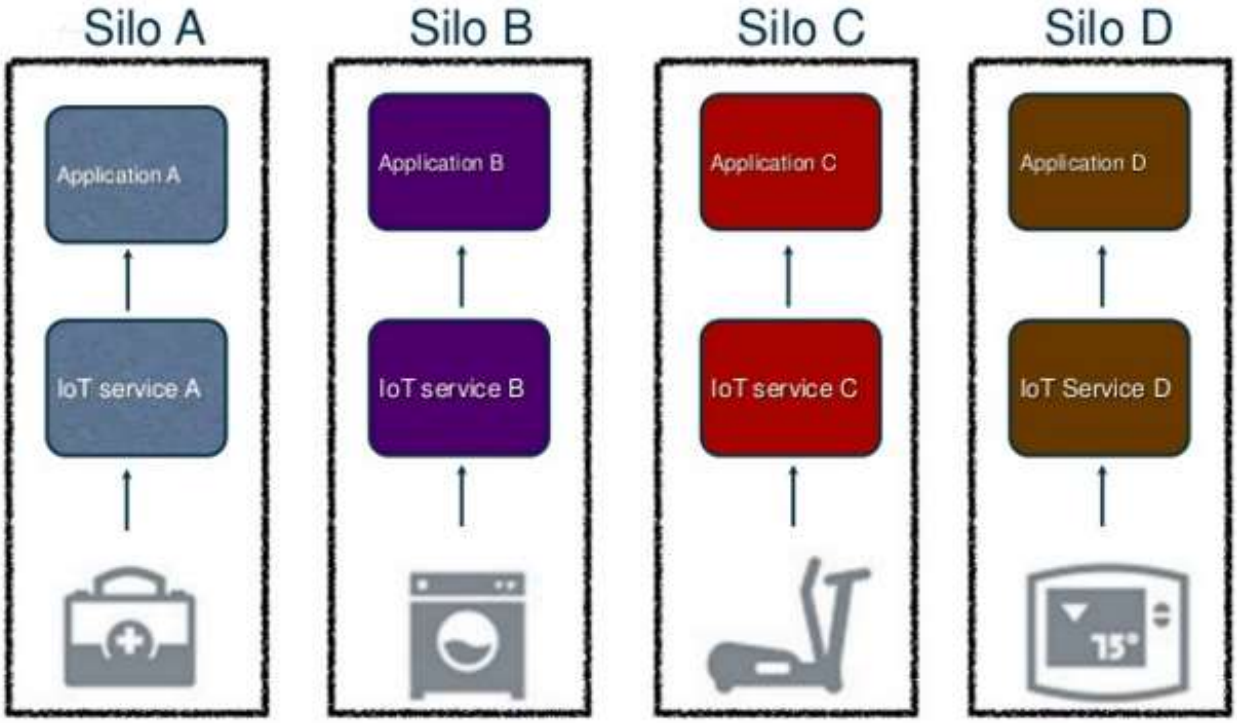
こうした状況が頻発してしまうと、本来 IoT で実現されるはずのさまざまなメリットが台無しになってしまい、ユーザが IoT 製品やサービスを利用するモチベーションが落ちてしまう。相互運用性が注目されるのは、こうした状況を回避するためであり、IoT に取り組む企業は業界団体などを通して相互運用ができるような標準仕様の策定に取り組んでいる。

そうした中、IoT 業界は現在、「IoT 標準規格戦争[10]」と呼ばれるような状況になってしまっており、業界には、単に業界団体が IoT の相互運用性を実現するための標準仕様を策定するだけでは十分ではないという声もある。ある関係者などは、「グローバルなスケールで IoT を成功させる鍵は、単一の標準規格（standard）にこだわることだ[11]」などとコメントしている。また、地理空間に関する情報の標準化を行っている OGC（Open Geospatial Consortium）で Interoperability Programs の Director を務めていた Raj Singh 氏（現在は IBM 社に所属）は、現在のようなプロプライエタリなセンサーデータ形式とサービスインタフェースでは IoT 業界はサイロ型を突き進むだけであり、そうなれば IoT ではなくなってしまうと、と指摘している。

以下の図表 6 は、Singh 氏が指摘するサイロ型の「IoT」の現状を示したものである。IoT 環境がサービスや機能ごとに独立してしまっており、特定のサービスや機能を跨いで連携しない仕組みとなっていることがわかる。

[10] http://www.datacenterknowledge.com/archives/2015/07/23/the-iot-standards-war/
[11] http://www.redbend.com/data/upl/whitepapers/Making Sense of IoT Whitepaper.pdf

図表 6：サイロ型になってしまっている現在の「IoT」



出典：SlideShare[12]

IoT 業界では既に相互運用性への取り組みが出てきていることから、ここまで極端な状態になることは想像しにくいが、現在は自らが IoT の基盤となるべく動いている企業も多数出てきており、主導権争いが進む中で、企業を軸としたサイロ型の IoT 市場が形成される可能性もある。

なお、自らが IoT の基盤となるべく動いている企業の代表例としてあげられるのが Google 社である。同社は 2015 年 5 月に開催したイベント Google I/O 2015 の基調講演において、Project Brillo と呼ばれる独自の IoT 基盤を発表した。Google 社が 2014 年 7 月にサーモスタットなどを開発している Nest Labs を買収したことを踏まえると、Android ベースの Brillo は今後、有力な IoT 基盤のひとつになり得る可能性を秘めており、Apple 社や Samsung 社など同様の取り組みを進めている他社があることなども考えると、企業の独自 IoT 基盤を軸にサイロ型の IoT 市場が形成される可能性もあると言える。

以下の図表 7 は、Google I/O 2015 の基調講演において Project Brillo を発表する Google 社の Sundar Pichai 氏である。

[12] http://www.slideshare.net/rajrsingh/iot-meets-geo

図表 7：Project Brillo を発表する Sundar Pichai 氏

出典：YouTube[13]

図表 6 で指摘されているようなサービスや機能を軸としたサイロ型の IoT 環境、各企業の独自 IoT 基盤を軸にしたサイロ型の IoT 環境を回避するためには、機器、製品、サービス、機能、企業の枠組みを超えて相互運用性を担保する IoT 基盤の登場と普及が欠かせない。その IoT 基盤を策定する役割を果たすのが、業界団体であり、今では複数の業界団体が相互運用性を実現するような IoT 基盤の策定に向けて動き出している。

（2） 注目すべき IoT 基盤

本項では、製造、自動車、スマートシティ/スマートハウス/住宅、医療・ヘルスケア、社会インフラなどの分野にフォーカスし、米国において各分野向け、そして分野横断型で確立されつつある代表的な IoT 基盤を抽出し、その動向を整理する。取り上げる IoT 基盤については、既存のさまざまな資料を参考にした上で選定した[14]。選定にあたっては、本レポートの冒頭で紹介した IoT 基盤の定義（IoT 機器をつなぐ時に利用出来るソフトウェアプラットフォームというもの）に基づき、ZigBee Alliance などのネットワークの相互運用性を目指すような業界団体は除外している。また、業界団体や標準化団体による取り組みにフォーカスし、先ほど紹介した Google 社の Brillo や Apple 社の HomeKit など、個別の企業によるプロプライエタリな IoT 基盤の開発・展開に向けた取り組みについても、今回の対象からは外している。

まず、本項で取り扱う IoT 基盤の一覧を以下の図表 8 にまとめる。取り扱うのは、①IIRA（Industrial Internet Reference Architecture）、②RVI（Remote Vehicle Interaction）、③Green Button、④Continua Design Guidelines、⑤OpenFMB、⑥oneM2M、⑦AllJoyn、⑧OCF、の 8 種類である。

[13] https://www.youtube.com/watch?v=uMt7UNvDGak
[14] http://www.redbend.com/data/upl/whitepapers/Making Sense of IoT Whitepaper.pdf
http://techbeacon.com/state-iot-standards-stand-big-shakeout
http://www.networkworld.com/article/2456421/internet-of-things/a-guide-to-the-confusing-internet-of-things-standards-world.html
http://www.slideshare.net/OpenViewVenturePartners/internet-of-things-presentation-45886299
http://postscapes.com/internet-of-things-alliances-roundup

図表 8：本レポートで取り上げる IoT 基盤一覧

IoT 基盤名	分野	団体名	概要	機能等	テストベッド	セキュリティ・セーフティ・信頼性規定
IIRA (Industrial Internet Reference Architecture)	製造（産業全般をカバー）	IIC	産業向け IoT の標準規格策定に影響を与えるためのレファレンスアーキテクチャ。	標準規格 ISO/IEC/IEEE 42010:2011 に基づいたフレームワーク。標準仕様策定の際などに利用されることを想定したレファレンスアーキテクチャという位置づけ。	産業向け IoT のユースケースに基づいたテストベッドを作成済み（現在 11 個）。	共通のセキュリティフレームワーク（セキュリティ、セーフティ、信頼性、回復性を検討）を作成しているほか、とテストベッドでもセキュリティを提供。
RVI (Remote Vehicle Interaction)	自動車	GENIVI Alliance	コネクテッド車輌間や他のデバイスやデータ交換を実現するためのオープンソースソフトウェアプラットフォーム（API ベースのアーキテクチャ）。	無線通信などを使い自動車で使われているソフトウェアのアップデートや遠隔からの自動車内の機器の操作などを実現。	情報なし。	これまでの認証と承認に向けた取り組みに加えて、RVI をセキュアで信頼性の高い、実証済みの技術とするべく取り組み中。
Green Button	スマートハウス（スマートシティにも応用可能）	Green Button Alliance	電力消費などの検針データをユーザがダウンロードし活用できるようにするための標準規格。	電力消費などの検針データのダウンロード機能、サードパーティーへのデータ統合機能などを提供。認証プログラムは現時点では前者のみカバー。	開発者が Green Button を利用したテストを自らで実施できるセルフテストページを公開。テストツールは NIST の協力のもと作成。テストや認証に関するドキュメントも公開中。	ユーザによるデータアクセス時には ID とパスワードでの認証によりセキュリティを担保。認証には OAuth 2.0 プロトコルを利用。
Continua Design Guidelines	医療・ヘルスケア	PCHA	ヘルスケア向けの機器やサービスの相互運用性を担保するためのガイドライン。	2013 年 12 月 19 日に ITU [15] が ITU-T H.810 として採用済み。機器同士の通信には IEEE 11073 を、医療情データ表現・交換する規格には HL7 を採用。	メンバーはテストツールを入手可能。また、製品の市場投入前に相互接続性テストを行うことなども可能。	規定されている各インターフェースで、アイデンティティマネジメント、同意のマネジメント、認証などによりセキュリティとプライバシーの課題に対応。
OpenFMB	社会インフラ	SGIP	分散電源など点在する電力関連情報を統合的に収集・管理するためのフレームワーク。	Modbus 、DNP3 、IEC 61850 などの標準規格を採用したアプリケーションに対応。さまざまな分散電源が採用している技術面の違いなどを意識することなく、分散	主要メンバー企業であるノースカロライナ州の電力事業者 Duke Energy 社、テキサス州の電力事業者 CPS Energy 社、研究所 NREL などがテスト	ネットワーク部分でセキュリティ対策を施している他、データを管理するホスト部分でもセキュリティ対策済み。

[15] ITU とは International Telecommunication Union の略で日本語名は国際電気通信連合。無線を含む電気通信分野において国際的な標準仕様・規格の策定、確立、普及などを中心とする活動を行う組織である。

				電源を柔軟に統合管理することが可能。	ベッドを提供。	
oneM2M	分野横断	oneM2M	M2M/IoT 関連のサービス層を定義したプラットフォームアーキテクチャ。	2015 年 1 月に発表された技術仕様リリース 1 では、アーキテクチャ内の共通サービス・エンティティ（CSE）において 12 種類の共通サービス機能を定義済み。	技術仕様リリース 1 の発表後に、仕様に準じて開発された機器同士の相互接続試験を実施。また第 2 回目の試験も予定済み。	技術仕様リリース 1 では、文書番号 TS-M2M-0003v1.0.1 においてセキュリティ技術をカバー。
AllJoyn	分野横断	AllSeen Alliance	IoT にかかるあらゆる機器やサービス間の相互運用性を担保するためのオープンソースなソフトウェアフレームワーク。	①AllJoyn アプリケーション層（ユーザエクスペリエンス）、②AllJoyn サービスフレームワーク（相互接続性）、③AllJoyn コアライブラリ（デバイス検出・接続、アクセスコントロール、暗号化など）、の三層構造でアーキテクチャを定義。	認証プログラムを提供済みであり、製品の相互接続性を認証。認証プログラムでは、一般向けの認証テストツールなども提供。	アプリケーションレベルでのセキュリティを提供。具体的には、認証とデータの暗号化をアプリケーションレベルで実行する仕組み。
IoTivity	分野横断	OCF	IoT にかかるあらゆる機器やサービスを相互接続するためのオープンソースなソフトウェアフレームワーク。	「Discovery（デバイスなどの検出）」、「Data Transmission（データ転送）」、「Device Management（デバイス管理）」、「Data Management（データ管理）」という 4 つの主要機能を提供。	テストベッドの存在は確認できず。ただし、現在認証プログラムを開発中であり、将来的に提供する予定。	セキュリティ、アイデンティティ、パーミッションなどをカバー。

出典：各種情報を基に作成

以下ではまず、各 IoT 基盤の概要と機能、その基盤の整備や運用を担当する標準化団体についての詳細に加え、各 IoT 基盤が提供するテストベッドやセキュリティ関連の規定の有無などを分野別に紹介する。なお、特定分野向けの IoT 基盤については、異分野の IoT 基盤との連携状況についても取り上げている。

（3） 製造分野の IoT 基盤：IIRA (Industrial Internet Reference Architecture)

a. IIRA (Industrial Internet Reference Architecture) の概要

Industrial Internet Reference Architecture とは、業界団体 IIC（Industrial Internet Consortium）によって作成されたレファレンスモデルである。IIC は 2014 年 3 月に設立されたコンソーシアムであり、米国マサチューセッツ州に拠点を置いている。設立メンバーには AT&T 社、Cisco 社、GE 社、IBM 社、Intel 社が名を連ねている[16]。

同コンソーシアムの FAQ[17]でも明示されているとおり、IIC は自らで新しい標準規格を策定することは意図していない。同団体の目的はあくまで、産業向けの IoT システム（IIC はこれを Industrial Internet

[16] http://www.iiconsortium.org/members.htm
[17] http://www.iiconsortium.org/faq.htm - accordion-18

System(IIS)と呼んでいる）に関するグローバルな標準規格の策定プロセスに影響を与えることである、としている。ここでいう「産業」とは、製造分野[18]以外にエネルギー分野[19]、ヘルスケア分野[20]、公共分野[21]、交通分野[22]を含んでいる[23]。

こうした意識のもと、IIC は IIRA と呼ばれるインダストリアル・インターネット向けのレファレンスアーキテクチャ[24]を作成している。IIC のさらなる特徴として、テストベッドに力を入れている点があげられる。IIC が提供しているテストベッドはさまざまな分野に対応しており、2016 年 3 月上旬時点では 11 のテストベッドが用意されていることが確認できている。

b. IIC の活動概要

前述のとおり、IIRA を作成する IIC は業界コンソーシアムであり、2014 年 3 月に設立されている。メンバー企業は、2015 年末時点で 27 カ国から集まった 230 社にのぼっている[25]。主な活動はワーキンググループで行われており、現時点では以下の 7 つのワーキンググループが存在している。

- ビジネス戦略およびソリューションライフサイクル
- 法律
- マーケティング
- メンバーシップ
- セキュリティ
- 技術
- テストベッド

このうち、レファレンスアーキテクチャである IIRA の作成を担当しているのは、技術ワーキンググループである。なお、IIC が最も力を入れているテストベッドについては、当然ながらテストベッドワーキンググループが担当している。

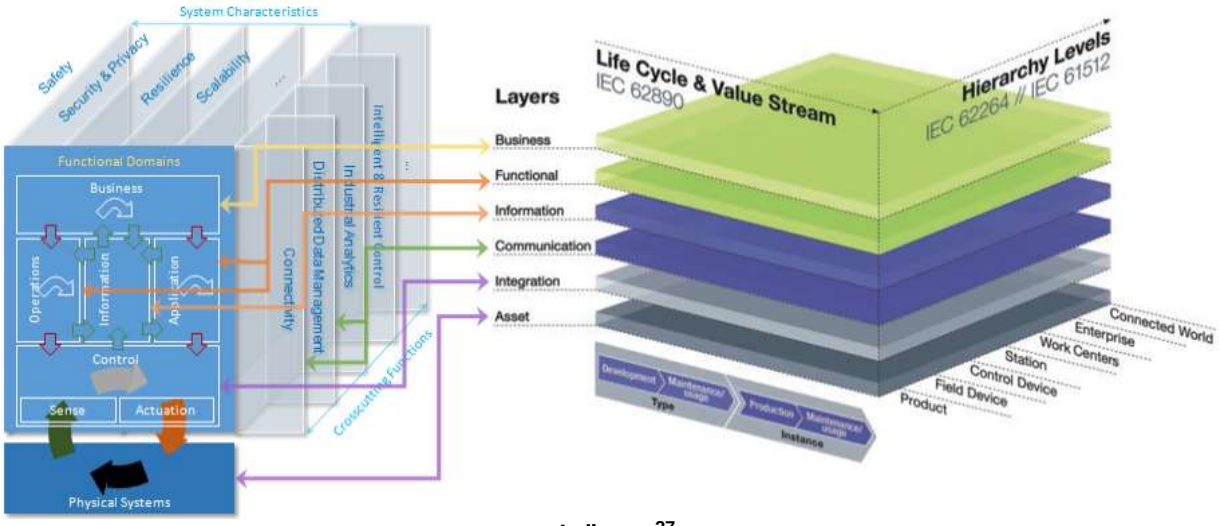
自らで標準規格を策定しない IIC は、実際に標準規格を策定する標準化団体や他の技術コンソーシアムと積極的な連携を図っている。そのうち、本レポートで紹介する団体としては OCF（Open Connectivity Foundation）や SGIP（Smart Grid Interoperability Panel）がある。

他団体との連携という点からの大きな動きとしては、2016 年 3 月 2 日に発表された業界団体 Platform Industrie 4.0 との協業[26]がある。この協業により、IIC のレファレンスアーキテクチャである IIRA と、Platform Industrie 4.0 のレファレンスアーキテクチャである RAMI4.0（Reference Architecture Model for Industrie 4.0）という 2 つのモデルがお互いに補完し合える体制が確立された。

以下の図表 9 は、IIRA と RAMI4.0 という 2 つのモデルがお互いに補完し合うことを示したものである。左側の図が IIRA、右側の図が RAMI4.0 を示している。

[18] http://www.iiconsortium.org/vertical-markets/manufacturing.htm
[19] http://www.iiconsortium.org/vertical-markets/energy-utility.htm
[20] http://www.iiconsortium.org/vertical-markets/healthcare.htm
[21] http://www.iiconsortium.org/vertical-markets/public-sector.htm
[22] http://www.iiconsortium.org/vertical-markets/transportation.htm
[23] このように多様な分野に対応しているため、本レポートの分野のくくりで言えば、分野横断型に近いコンソーシアムという見方もできるが、後述するように、先日ドイツの製造分野向けのコンソーシアムである Industrie4.0 との協業を発表していることから、製造分野の分類として紹介している。
[24] http://www.iiconsortium.org/IIRA.htm
[25] http://blog.iiconsortium.org/2015/12/2015-the-year-things-came-together.html
[26] http://www.iiconsortium.org/press-room/03-02-16.htm

図表 9：IIRA と RAMI4.0 の補完関係



出典：IIC[27]

両団体の協業はこれにとどまらず、今後は IIC の テストベッドと Platform Industrie 4.0 のテスト設備基盤を連携させる可能性なども模索していくとされている。

なお、IIC の創設企業の一社である GE 社の Greg Petroff 氏は両団体の連携について、「技術を軸としたサイロ型の IoT アーキテクチャを打ち砕き、これらアーキテクチャ活動のより適切な統合を支援することは、産業インターネットの発展にとっての鍵です。今回の連携は、世界最大の課題の解決に向けて統合を加速する標準をベースに、活発で統一されたコミュニティーの構築に貢献していくはずです[28]」とコメントし、この連携が産業向けの IoT の取り組みとして重要なものであることを強調している。

c. IIRA の機能

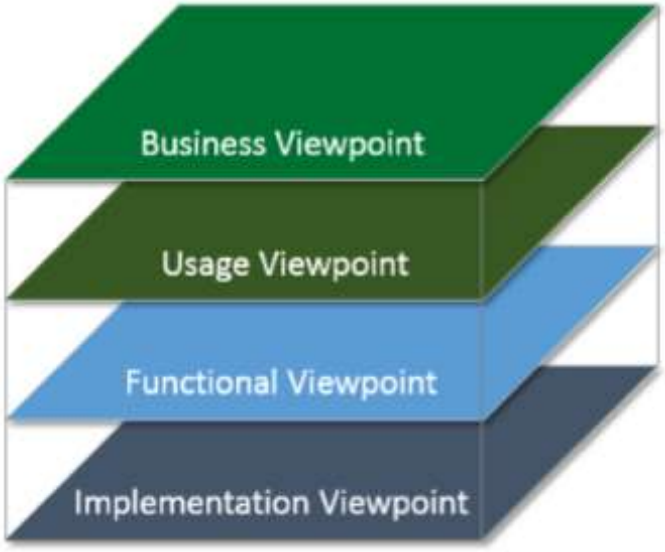
冒頭の概要でも紹介したとおり、IIRA を作成している IIC は、特定の標準規格を策定することを目的としていない。その代わりに、同団体が力を入れているのがレファレンスアーキテクチャの作成と後述するテストベッドである。

このレファレンスアーキテクチャは、細かい仕様を定める際の議論に活用できるアーキテクチャフレームワークを示すもの、と位置づけられており、標準規格である ISO/IEC/IEEE 42010:2011[29]に基づいたフレームワークとなっている。なお、本レポート執筆時点で、一般に入手できる IIRA は 2015 年 6 月 4 日付のバージョン 1.7 となっている。

なお、IIC はアーキテクチャフレームワークを検討するにあたり、図表 10 に示す Business、Usage、Functional、Implementation という 4 つの観点から検討を行ったとしている。

[27] http://blog.iiconsortium.org/2016/03/the-industrial-internet-is-important-new-technologies-and-new-business-opportunities-will-disrupt-industries-on-many-level.html
[28] http://www.zaikei.co.jp/releases/336136/
[29] http://www.iso.org/iso/catalogue_detail.htm?csnumber=50508

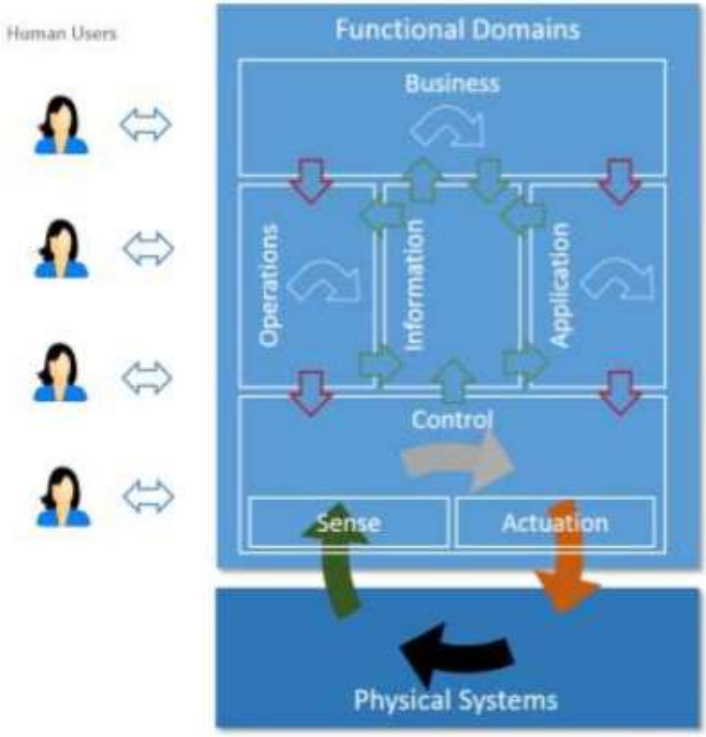
図表 10:アーキテクチャフレームワーク検討の観点



出典:IIC[30]

例えば、下から 2 層目に当たる Functional(機能面)を検討する上では、図表 11 に示す 5 つのドメイン、すなわちビジネス、運用、情報、アプリケーション、制御というドメインに分解した上で、それぞれのドメインに求められる要素を特定している。

図表 11:アーキテクチャフレームワーク検討の観点



出典:IIC

[30] http://www.iiconsortium.org/IIRA.htm
※上記より登録後にダウンロードできる"The Industrial Internet Reference Architecture Technical Report"を参照。

なお、異分野の IoT 基盤との連携という点については、IIRA はそもそも製造分野に限らず、産業向け IoT のさまざまな分野への対応を目指しているレファレンスアーキテクチャであり、製造分野以外にもインダストリアル・インターネット全般をカバーしている。

d. IIC のテストベッド

IIC では自ら標準規格を策定しない代わりに、テストベッドの作成に力を入れている。作成の中心となっている IIC のテストベッドワーキンググループは、IIC のメンバー企業からテストベッドに関する意見を募り、その有用性や実現可能性を厳密に確認した上で、実際に利用できるものとして公開している。図表 12 は現在公開されているテストベッドの名称と各テストベッドの主担当企業（リードメンバー）を示している。

図表 12：アーキテクチャフレームワーク検討の観点

テストベッド名	主担当企業
資産効率テストベッド[31]	Infosys
マイクログリッドアプリケーションのための通信と制御テストベッド[32]	RTI、National Instruments、Cisco
状況監視と予知保全テストベッド[33]	IBM、National Instruments
エッジインテリジェンステストベッド[34]	HP Enterprise、RTI
工場運用の見える化とインテリジェンスのためのテストベッド[35]	富士通、Cisco
高速ネットワークインフラテストベッド[36]	GE
IDT（インダストリアル・デジタル・スレッド）テストベッド[37]	Infosys、GE
INFINITE（INternational Future INdustrial Internet）テストベッド[38]	EMC、コーク工科大学
セキュリティクレーム評価テストベッド[39]	Xilinx、UL、Aicas、PrismTech
TSN（Time-Sensitive Networking）テストベッド[40]	Bosch Rexroth、Cisco、Intel、KUKA、National Instruments、Schneider Electric、TTTech
追跡（Track and Trace）テストベッド[41]	Bosch、Cisco、National Instruments、TechMahindra

出典：IIC[42]

e. IIRA のセキュリティ

IIRA のセキュリティについては、IIC のセキュリティワーキンググループが取り組んでおり、その具体的な取り組み内容を公開している[43]。資料によると、IIC ではインダストリアル・インターネットのセーフティ、リライアビリティ、セキュリティに取り組んでいると前置きした上で、具体的な取り組みについて次の 2 点を紹介している。

まず 1 点目は、共通セキュリティフレームワークの作成である。これはインダストリアル・インターネットで実装されるシステムの特徴を踏まえ、さまざまな分野（具体的には産業分野、情報分野、制御分野、分析分野、

[31] http://www.iiconsortium.org/asset-efficiency.htm
[32] http://www.iiconsortium.org/microgrid.htm
[33] http://www.iiconsortium.org/cm-pm.htm
[34] http://www.iiconsortium.org/edge-intelligence.htm
[35] http://www.iiconsortium.org/fovi.htm
[36] http://www.iiconsortium.org/high-speed-network.htm
[37] http://www.iiconsortium.org/industrial-digital-thread.htm
[38] http://www.iiconsortium.org/infinite.htm
[39] http://www.iiconsortium.org/security-claims.htm
[40] http://www.iiconsortium.org/time-sensitive-networks.htm
[41] http://www.iiconsortium.org/track-and-trace.htm
[42] http://www.iiconsortium.org/wc-testbeds.htm
[43] http://www.iiconsortium.org/pdf/IIC_Approach_to_Securing_Industrial_Internet_Systems.pdf

クラウド分野）のセキュリティの用語を統合して整理している。そして 2 点目は、IIC が公開しているテストベッドのセキュリティである。

このような内容を踏まえ、IIRA の資料[44]では第 8 章でセーフティについて、第 9 章ではセキュリティと信頼性、そしてプライバシーについて扱っている。また続く第 10 章では回復性（Resilience）についても取り上げている。このうち、第 9 章のセキュリティについては特に詳細な記述がある（残る第 8 章、第 10 章は数ページの分量）。セキュリティの章では要素ごとに分類したセキュリティを取り上げており、具体的にはエンドポイント、通信、管理と監視、そしてデータ配信と蓄積の 4 分野に分けてセキュリティを検討している。

（4） 自動車分野の IoT 基盤：RVI (Remote Vehicle Interaction)

a. RVI の概要

RVI（Remote Vehicle Interaction）とは、業界団体 GENIVI Alliance[45]が 2015 年 11 月 16 日～18 日にロサンゼルスで開催された業界会議 Connected Car Expo[46]で発表したオープンソース・ソフトウェア・プラットフォームのことである[47]。

GENIVI Alliance とは、オープンソース型の車載インフォテインメント（IVI：In-Vehicle Infotainment）向けソフトウェアの普及を目指すアライアンスである。同アライアンスはインフォテインメント製品を開発する自動車メーカーにオープンソースのソリューションを採用してもらうことを目的に活動しており、これまでレファレンスアーキテクチャ、ソフトウエアコンポーネント、標準インターフェースなどを提供してきた。

同団体は当初は単に車輌のコネクティビティーだけを考えていたが、今ではさまざまな種類のデバイスとの接続までを検討するという IoT 的な視点までを活動範囲としている。これは、GENIVI Alliance が CES 2016 開催中にサブ会議 Consumer Telematics Show の基調講演をすることが決まった際に、そのことを伝えたプレスリリースにおいて、「真のコネクテッド車両を実現できるかどうか、単にコネクティビティーだけでなく、自動車やその他のデバイス、サービス、その他の自動車との間で、容易、確実、そして安全な方法でデータ交換できる仕組みにかかっていると認識した[48]」としていることからもわかり、同団体は自動車向けの IoT 基盤の重要性を訴えるようになっている。このようなコメントを踏まえ、GENIVI Alliance は同アライアンス内に正式に RVI 専門グループを立ち上げることを発表している[49]。

なお、この RVI 専門グループが取り組む RVI であるが、Linux Foundation 内の自動車向けソリューションに特化したワーキンググループ Automotive Grade Linux において Jaguar Land Rover 社が 2013 年から開発してきたものを引き継いだものとなっている。

b. GENIVI Alliance の活動概要

GENIVI Alliance はオープンソースの IVI の普及を目的として 2009 年 3 月に設立された業界団体である。設立メンバーには、BMW Group 社、GM 社、Delphi 社、Intel 社、Magneti-Marelli 社、PSA Peugeot Citroen Delphi 社、Visteon 社、Wind River Systems 社といった企業が名を連ねている[50]。

---

[44] http://www.iiconsortium.org/IIRA.htm
※上記より登録後にダウンロードできる”The Industrial Internet Reference Architecture Technical Report”を参照。
[45] http://www.genivi.org/
[46] http://connectedcarexpo.com/
[47] http://www.genivi.org/sites/default/files/press-releases/english/2015_11_12_CCE_Final_Release.pdf
https://prw.kyodonews.jp/opn/release/201511135611/
[48] https://prw.kyodonews.jp/opn/release/201512226696/
[49] http://www.genivi.org/newsletter - mctoc2
[50] https://en.wikipedia.org/wiki/GENIVI_Alliance

現在、同アライアンスの会長を務める Matt Jones 氏は、Jaguar Land Rover 社で先見性のある技術（Future Technology）を扱う部門の Director も務めている[51]。同氏は 2015 年に開催された TU-Automotive において「その年に最も影響力がある人」に選ばれており[52]、自動車業界における最新テクノロジ分野を牽引する人物の 1 人である。図表 13 は 2015 年に東京で開催された Automotive Grade Linux でプレゼンテーションをする Matt Jones 氏である。

図表 13：Matt Jones 氏

出典：LWN.net[53]

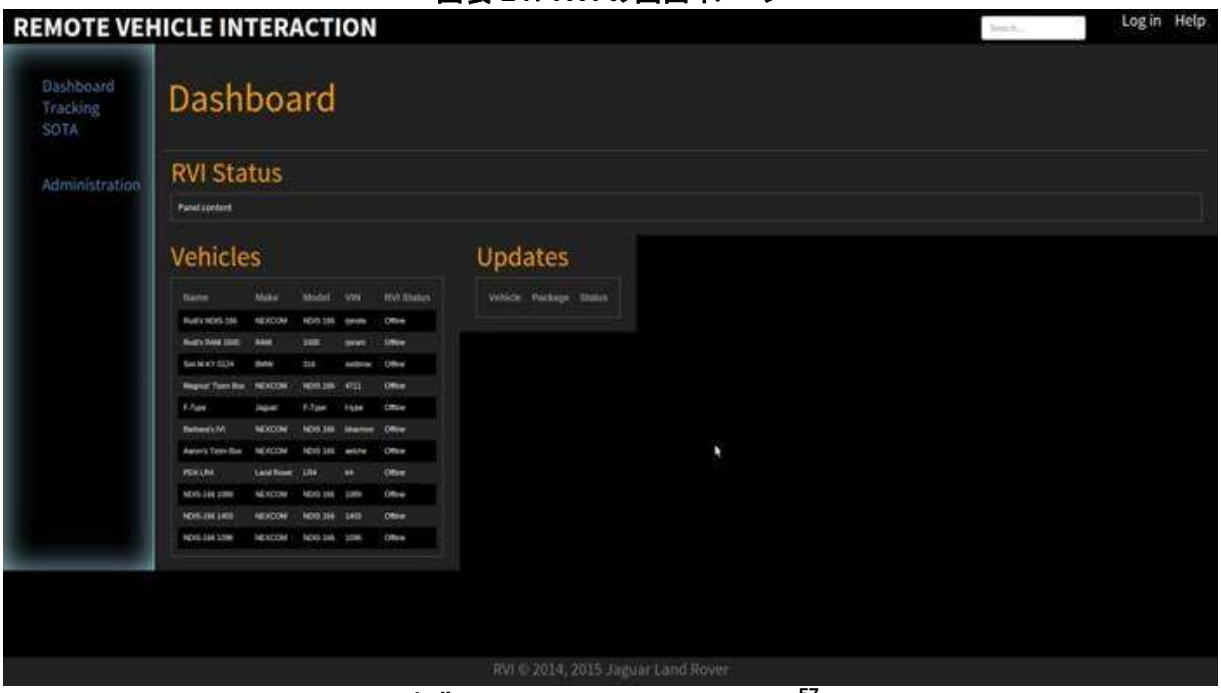
なお、GENIVI Alliance は上記の通り、これまでは IVI の普及を目的に、オープンソースベースの IVI 向けリファレンスアーキテクチャ[54]の策定を中心に活動してきた。2015 年 1 月には、このオープンソースベースのソリューションの普及を広げるため、Google 社が開発を進める車載用プラットフォーム Android Auto に対応したオープン・インタフェースを提供することなども発表している[55]。

c. RVI の機能

GENIVI Alliance が策定する RVI（Remote Vehicle Interaction）は、もともとは Linux Foundation 内の Automotive Grade Linux におけるプロジェクト[56]として Jaguar Land Rover 社のメンバーが中心となって開発を進めていたものである。同プロジェクトは、次世代のコネクテッド車輌サービスの開発を加速させるようなインフラのリファレンス実装を設計・開発する目的として立ち上げられた。以下の図表 14 は同プロジェクトで開発された RVI のリファレンス実装の画面イメージである。

[51] http://www.genivi.org/board-and-officers
[52] http://www.genivi.org/sites/default/files/press-releases/english/GENIVI Alliance President Named TU-Automotive Influencer of the Year~Final Release.pdf
[53] http://www.iiconsortium.org/wc-testbeds.htm
[54] http://www.genivi.org/sites/default/files/resource_documents/GENIVI_Reference_Architecture_29Oct2015.pdf
[55] http://www.genivi.org/sites/default/files/press-releases/japanese/GENIVI Alliance to Provide Android Auto Interface Final Release_JPN.pdf
[56] https://wiki.automotivelinux.org/eg-rvi

図表 14：RVI の画面イメージ



出典：Automotive Grade Linux[57]

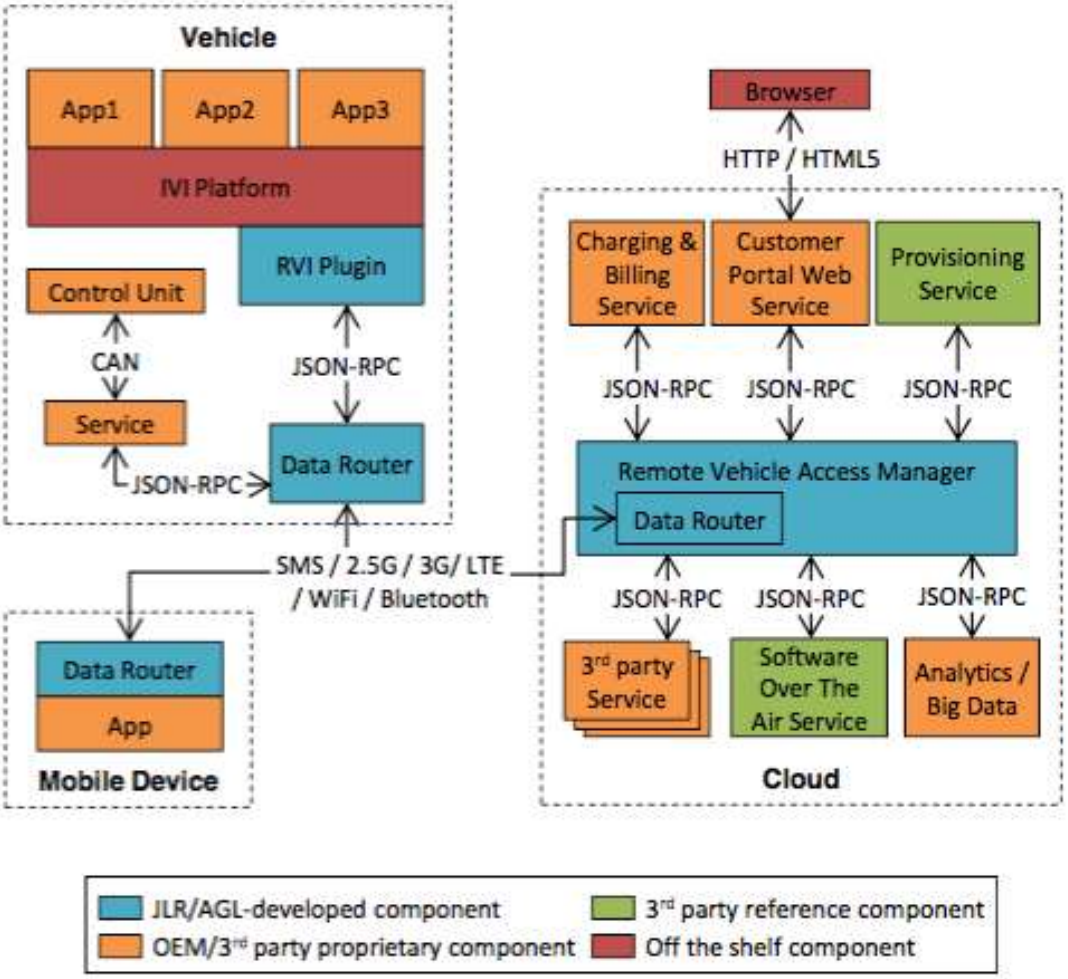
現在では上記の通り、GENIVI Alliance の RVI 専門グループがこれを Automotive Grade Linux より引き継いでおり、RVI 専門グループが普及にあたっている。RVI 専門グループの主要メンバー企業としては、Jaguar Land Rover 社、Ericsson 社、Arynga 社、Automotive Grade Linux が名を連ねている。現時点では自動車メーカーは少ないが、今後は Toyota 社、P3 Group 社、Konsulko Group 社なども主要メンバーとして加わる可能性があるとされている[58]。

この RVI であるが、上記でも紹介した 2015 年開催の業界会議 Connected Car Expo において Jaguar Land Rover 社の RVI 搭載車輌（F-TYPE コンバーチブル）が展示され、正式に発表された。単に車輌を展示するだけでなく、リモート･データ･ロギング（遠隔からのデータの抽出）、無線通信経由のセキュアなソフトウエアアップデート、スマートフォンアプリを使った温度調節といったサービス機能のデモンストレーションなども行われている[59]。

このような機能を実現できる RVI は、API ベースのアーキテクチャとして設計されている。図表 15 は Automotive Grade Linux での RVI 開発プロジェクトにおいて検討された RVI のアーキテクチャである。現在もこのアーキテクチャを引き継いでいる。

[57] https://wiki.automotivelinux.org/eg-rvi
[58] http://www.genivi.org/newsletter - mctoc2
[59] http://www.genivi.org/sites/default/files/press-releases/english/2015_11_12_CCE_Final_Release.pdf

図表 15: RVI のアーキテクチャ



出典: Automotive Grade Linux[60]

今後、GENIVI Alliance 内の専門グループとして活動をしていくにあたっては、RVI をセキュアで信頼性の高い、実証済みの技術として認められることを目的としていくとしている。

なお、異分野の IoT 基盤との連携という点については、今のところ具体的な情報はない。

d. RVI のテストベッド

RVI のテストベッドについては、Automotive Grade Linux の情報としても、新しい GENIVI Alliance の情報としても明示されていない。

e. RVI のセキュリティ

RVI のセキュリティに関しては、Automotive Grade Linux のプロジェクトのスコープとして、認証と承認が含まれている[61]。また、GENIVI Alliance 内の RVI 専門グループの活動方針として、RVI をセキュアで信頼性の高い、実証済みの技術として認められるよう取り組んでいくということが明示されている。

[60] https://wiki.automotivelinux.org/_media/eg-rvi/remote_vehicle_interaction_agl_presentation_2014-16-18_rev2.pdf
[61] https://wiki.automotivelinux.org/eg-rvi/technical_scope

（5） スマートハウス分野の IoT 基盤：Green Button

a. Green Button の概要

Green Button とは、米国の電力事業者がスマートメーター経由で計測している電力消費データを、顧客が自由に利用することができる仕組みを提供する取り組みである。利用するにあたっては、特別なソフトウェアなどを利用することなく、シンプルな共通フォーマットでダウンロードできることが求められている。

この取り組みは 2011 年 9 月に米国で開催されたスマートグリッドイベントである GridWeek[62]において、連邦政府の初代 CTO である Aneesh Chopra 氏が電力業界に対して取り組みを促したことで始まった。以下の図表 16 は、GridWeek で講演する Aneesh Chopra 氏である。

図表 16：GridWeek でプレゼンテーションする Aneesh Chopra 氏

出典：GridWeek[63]

その後、GreenButton の取り組みは、NIST の元でスマートグリッド関連の標準化策定に取り組んでいた SGIP（Smart Grid Interoperability Panel）が主導する形で進められることなった。具体的な技術面での開発は NAESB（北米エネルギー企画委員会）が担当し、同委員会の ESPI（Energy Services Provider Interface）[64]を中心に Green Button の規格が定められた。

ただし、2015 年に Green Button 規格の管理等が Green Button Alliance に移管されており、現在では同アライアンスが GreenButton の取り組みを管理する形となっている。なお、既にさまざまな電力事業者が Green Button を活用している。

b. Green Button Alliance の活動概要

Green Button Alliance は、SGIP の活動を引き継ぐ形で 2015 年に設立された業界団体である[65]。同アライアンスの議長（Chair）はカナダの電力事業者 London Hydro 社の Syed Mir 氏であり、副議長はカリフォルニア州の電力事業者 Southern California Edison 社の Mark Podorsky 氏が務めている。その他、米国の主要な電力事業者の幹部や出身メンバー、北米以外の電力事業者として初めて Green Button に対応したイタリアの Enel Group 社の Livio Gallo 氏などがボードメンバーに名を連ねている。

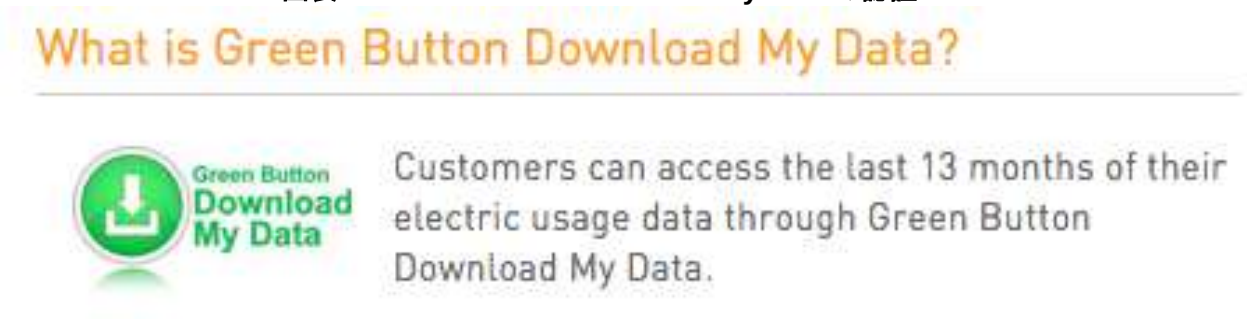
[62] http://www.gridweek.com/2011/
[63] http://www.gridweek.com/2011/
[64] https://www.naesb.org/ESPI_Standards.asp
[65] https://www.whitehouse.gov/blog/2015/07/22/green-button-initiative-makes-headway-electric-industry-and-consumers

Green Button Alliance に参加している企業や団体は、2016 年 3 月上旬時点で 100 社/団体にのぼっており、加盟する電力事業者が抱える顧客総数（家庭・法人両方）は 6,000 万以上であるとのことである。つまり、現在では北米を中心に少なくとも 6,000 万の世帯や法人が Green Button のソリューションを利用できる状態となっている。同アライアンスの活動の中心は、その設立目的からも Green Button の開発や展開である。具体的には、事業者による Green Button への取り組みを認証する認証機関としての活動、GreenButton のマーケティング活動、教育啓蒙活動などがある。

この中でも特に Green Button Alliance が積極的に取り組んでいるのは、認証活動である。ただし、現在のところは、Green Button を通して利用できる 2 種類のソリューション”Download My Data (DMD)”と”Connect My Data (CMD)”のうち、DMD を対象とした認証しか行われていない。なお、現在この認証を受けることができるのは、ユーザ（個人・法人問わず）にエネルギー関連サービス（現在は電力のみであるが、将来的にガスや水への対応も検討している）を提供している企業（Green Button Alliance の用語では Data Custodian と呼ばれるプレーヤ）であり、ユーザが自身のエネルギー消費データをダウンロードすることを許可する企業となる。

Green Button の認証を受けているユーティリティのウェブサイトを見ると、以下の図表 17 のように、文字どおり緑の認証ロゴが表示されている場合が多い。

図表 17：Green Button Download My Data の認証ロゴ



出典：PG&E[66]

c. Green Button の機能

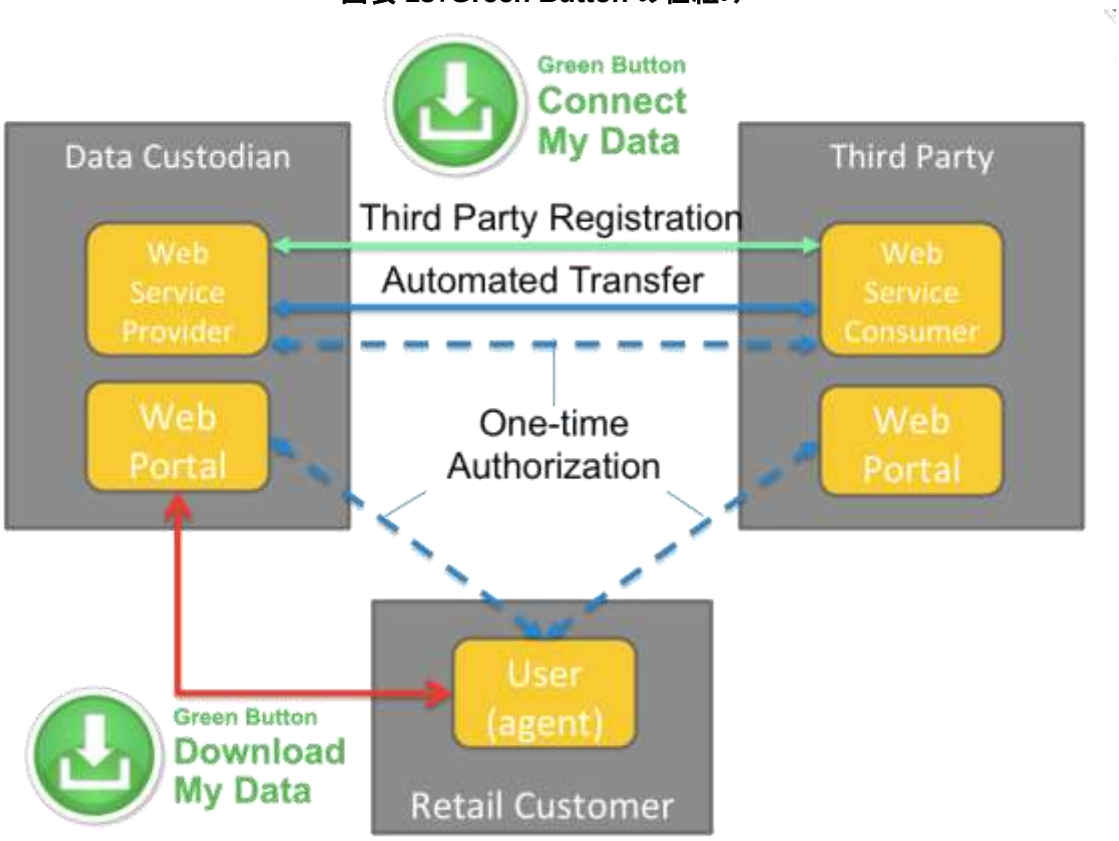
Green Button は RESTful API を利用して、電力やガス、水道などの検針データにアクセスできるようにするための仕組みである。関連するプレーヤとしては、Retail Customer、Data Custodian、Third Party の 3 種類がある。電力などのエネルギーを利用するユーザを Retail Customer と名づけている。この中には家庭向けのユーザだけではなく、商業施設や産業施設などの利用者も含まれている。電力事業者などユーザのデータを保持しているのが Data Custodian（文字どおり「データ管理者」）である。最後に、そのどちらにも属さないのが Third Party とある。

この Green Button で実現するのは上記の通り、DMD と CMD の 2 種類の機能である。このうち DMD ソリューションは、Retail Customer が電力事業者などの Data Custodian から直接データをダウンロードできるような仕組みを指している。一方の CMD については、Third Party のウェブサービスに Data Custodian からのデータが渡され、Retail Customer が Third Party のウェブポータル上でデータを確認できるようにするものである。認証プログラムについては、現時点では DMD のみが対象となっている。

以下の図表 18 は、Green Button の仕組みを表したものである。

[66] http://www.pge.com/en/myhome/addservices/moreservices/greenbutton/index.page

図表 18：Green Button の仕組み



出典：Green Button Alliance[67]

このような Green Button を経由してダウンロードするデータは XML 形式となっている。データの配信には Atom フォーマットが利用されている。

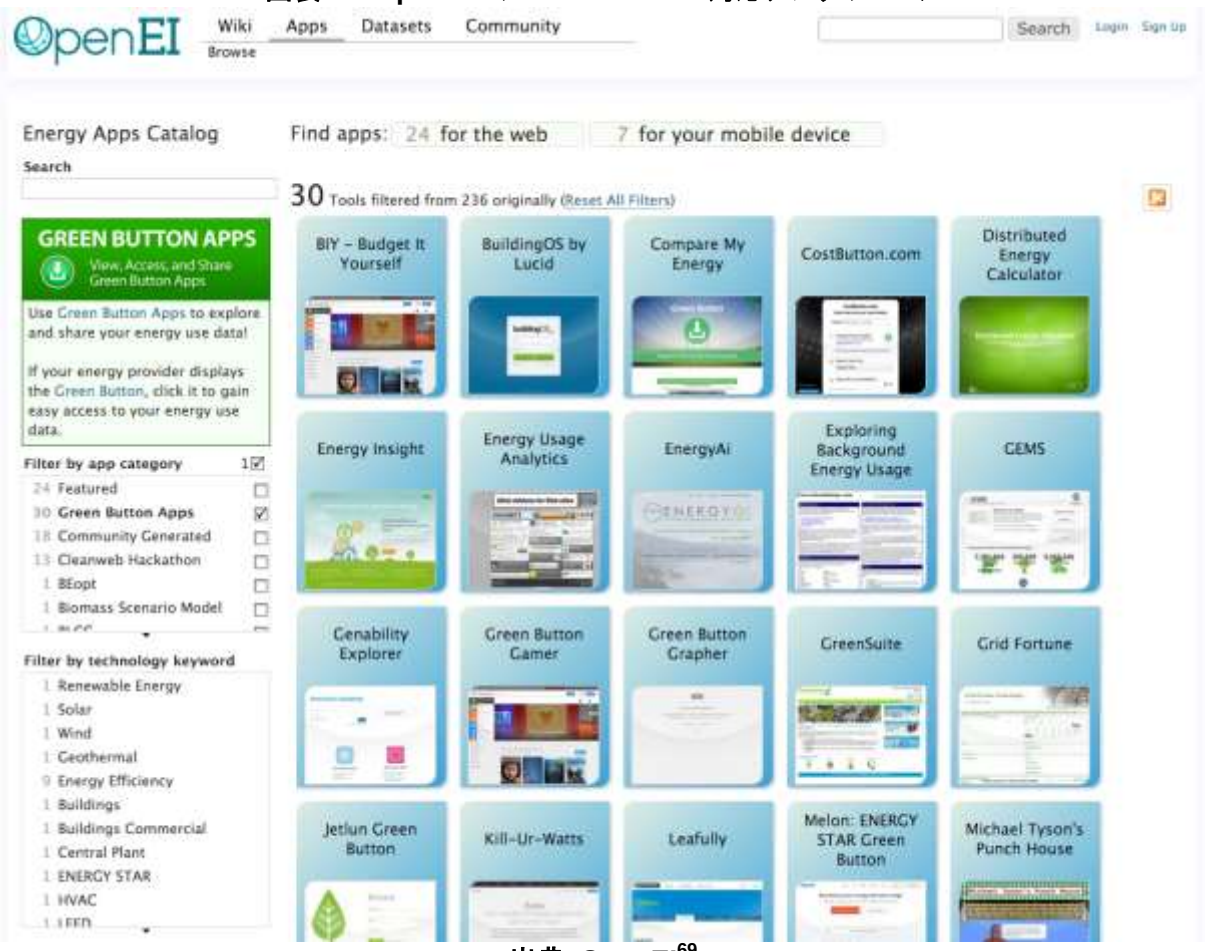
なお、Green Button はデータ仕様を定めるだけであり、ダウンロードできるデータの内容については各電力事業者の設定に委ねられている。理論的には、ユーザのエネルギー利用データを 15 分、1 時間、1 日、そして 1 ヶ月という単位でダウンロードすることができるが、具体的にどのような情報が含まれるかについては電力事業者によって異なる。

ユーザがダウンロードした XML 形式のデータをどのように活用するのかについては、Green Button Alliance のウェブページでは明示されていない。対応している電力事業者のウェブページを見ても、実際のユーザでなければそのデータをどのように活用するのかはわかりにくく、詳細は確認できなかった。

ただし、米国のエネルギー省に属する研究機関である NREL（国立再生可能エネルギー研究所）が管理する OpenEI（Open Energy Information）[68]というウェブページの中で、Green Button に対応したアプリが公開されており、ここから活用方法を窺い知ることが可能である。以下の図表 19 は、OpenEI の Green Button 対応アプリのページである。

[67] http://www.greenbuttondata.org/developers/
[68] http://en.openei.org/wiki/Main_Page

図表 19：Open EI の Green Button 対応アプリのページ



出典：OpenEI[69]

とはいえ、このウェブページは Green Button に対応する電力事業者の顧客に広く知れ渡っているとは言えない。Green Button の価値を最大限に活かすためには、Green Button そのものだけではなく、活用方法も合わせて伝えていくような啓蒙活動が必要と言える。

なお、Green Button Alliance は今のところ、異分野の IoT 基盤との連携については特に明示していない。ただし、データを電力事業者からダウンロードできる DMD だけではなく、今後、認証プログラムが開始される CMD の利用が進めば、サードパーティーがエネルギー消費情報に加えてあらゆるユーザ情報を一箇所に集めて管理・配信するアグリゲーションサービスに乗り出す可能性が考えられ、将来的には他のデータとの連携に向けた取り組みは十分にありえる。

特にスマートシティ分野については、北米以外で初めて Green Button を採用したイタリアの電力事業者 Enel Group 社がスマートシティプロジェクト L'Aquila smart city で Green Button を採用していることからもわかるように[70]、Green Button そのものがスマートシティ分野をカバーしていく可能性がある。同社の L'Aquila smart city プロジェクトでは、消費者は Green Button 経由でエネルギー消費データをリアルタイムにダウンロードできるほか、自身で選定したソフトウェアやアプリケーションで自由にデータを処理できるようになっているという。

[69] http://en.openei.org/apps/?keyword=Green Button Apps
[70] http://enel.ru/en/events_and_news/news/15111/

d. Green Button のテストベッド

Green Button Alliance は、開発者が Green Button にかかる必要なテストを自ら行えるようなセルフテストページを公開している[71]。ここで公開されているテストツールは、NIST の協力で作成されたものであるという。また、このテストツールの他にも、Green Button のドキュメントライブラリ[72]において、テストや認証に向けて参考となる文書（例えば DMD のテストプランをまとめた文書など）が公開されている。この参考文書主に Word ファイル形式となっており、誰もが自由にダウンロード可能である。

e. Green Button のセキュリティ

Green Button のセキュリティに関しては、同アライアンスの FAQ[73]に書かれているように、ユーザ自らがユーティリティなどのウェブポータルにログインする際にログインとパスワードなどで認証をすることで担保されているとしている。認証については OAuth 2.0 プロトコルを活用しているという[74]。

（6） 医療・ヘルスケア分野の IoT 基盤: Continua Design Guidelines

a. Continua Design Guidelines の概要

Continua Design Guidelines[75]とは、相互運用性を担保しながら各消費者にあったコネクテッドヘルス関連機器やソリューションを開発するための実装フレームワークであり、Continua Health Alliance[76]によって策定されている。この Continua Health Alliance はもともと 2006 年に設立された独立団体であったが、2014 年に他の 2 団体と合併する形で PCHA（Personal Connected Health Alliance）[77]が創設されたため、現在では PCHA のメンバー組織という位置づけにある。そのため、現在 Continua Design Guidelines を管理するのは PCHA である。

Continua Design Guidelines は、実績のある標準化団体によって策定された国際標準規格に基づく実装フレームワークであり、相互運用性を担保した柔軟なガイドラインとなっている点が特徴である。企業などはコネクテッドヘルス関連機器などの開発時にこのガイドラインに従うと、ベンダー固有の環境にとらわれない相互運用性のある機器やソリューションを開発することが可能となる。

なお、このガイドラインは、基本的には PCHA（Personal Connected Health Alliance）および Continua Health Alliance のメンバーでなければ確認できず、一般には公開されていない。

b. PCHA の活動概要

上記の通り、Continua Design Guidelines を策定したのは Continua Health Alliance であるが、同アライアンスは他の団体と共に PCHA を設立しており、現在では Continua Design Guidelines も PCHA のもとで管理されている。Continua Design Guidelines を巡る動きを活動団体の視点から時系列でみていくと、以下のようになる。

まず、Continua Health Alliance は 2006 年 6 月に設立されている。アライアンスのボードメンバー企業としては、富士通、Intel、Oracle、Orange、Philips、Qualcomm、Roche Diagnostics、シャープ、UnitedHealth Group などである[78]。2006 年 11 月には日本企業 6 社が地域委員会を設立し、2009 年には Continua

[71] http://www.greenbuttondata.org/greentest.aspx
[72] http://www.greenbuttondata.org/library/
[73] http://www.greenbuttondata.org/faq/
[74] http://www.greenbuttondata.org/developers/
[75] http://www.continuaalliance.org/products/design-guidelines
[76] http://www.continuaalliance.org/
[77] http://www.pchalliance.org/
[78] https://en.wikipedia.org/wiki/Continua_Health_Alliance - cite_note-BoardofDirectors-9

Design Guidelines の日本語版なども発表されている。同団体は独立した団体として活動していたが、2014 年 4 月 22 日に mHealth Summit[79]、HIMSS（Healthcare Information and Management Systems Society）[80]とともに PCHA（Personal Connected Health Alliance）[81]を設立したことで、現在では PCHA 傘下のアライアンスという位置づけにある。

この PCHA であるが、ICT 技術による健康増進と豊かな暮らしを実現するには、各団体が持つ有形・無形の資産を活用することが不可欠であるとの考えのもと、各団体が合併する形で設立された。ヘルスケア機器をプラグアンドプレイ形式で利用しながら、自分の健康データにアクセスできるような環境を確立することが活動目標となっている[82]。また、ヘルスケア分野でビッグデータを効果的に活用できるような技術の開発なども進めていくという

PCHA における Continua Health Alliance の役割については、「策定したガイドラインや機器認証プログラムに基づき、ヘルスケア機器の相互接続性と互換性を向上できるよう、業界標準の策定作業を進めること[83]」となっている。4 人いる PCHA のリーダーシップメンバー[84]のうち 2 人が Continua Health Alliance のメンバーであることを考えると、PCHA における Continua Health Alliance の重要性は高いと言える。

このように Continua Health Alliance は PCHA の中で中心的な役割を担っているが、現在では Continua Health Alliance そのものに新たに参画することはできず、Continua Design Guidelines にかかる活動への関与を希望する企業は PCHA へ参画する形となる。Continua Health Alliance の参加ページにアクセスしても、PCHA のメンバーになることを勧めるメッセージが表示される。PCHA のメンバーになることで、Continua Design Guidelines などのリソースにもアクセスできる形となっている[85]。

なお、PCHA は 2016 年 3 月 3 日に、後ほど紹介する AllSeen Alliance とのパートナーシップを発表している[86]。プレスリリースの中で、AllSeen Alliance は Continua Design Guidelines の重要性を認識しており、業界におけるリーディングカンパニーは今後 Continua Design Guidelines の発展に貢献していくことになると述べている。なお、AllSeen Alliance と PCHA には共通の企業が多く参加しており、この具体例としては Philips 社、IBM 社、Qualcomm 社、パナソニックなどがある。

c. Continua Design Guidelines の機能

Continua Design Guidelines は、冒頭でも紹介したように、相互運用性を担保しながら各消費者にあったコネクテッドヘルス関連機器やソリューションを開発するための実装フレームワークとなっている。既存の標準規格団体によって定められた標準規格を組み合わせた形のガイドラインであり、これを採用するメリットは次のようなものとなる。

例えば、コネクテッドヘルス関連機器を開発する際には、標準化されている複数の規格や仕様に従うことで、標準的な機器を開発できるが、各規格の信頼性を担保したまま相互接続できるようにするのは難しい。そこで、各規格の信頼性を担保したまま相互接続できるようにするための実装ガイドラインとして Continua Design Guidelines が機能する。また、同ガイドラインにもとづくアーキテクチャ（以下参照）を提示しており、これを実現する上で、各標準規格において対応が不要なものを特定したり、逆に追加的な対応を図るべきものを特定したりもしている。

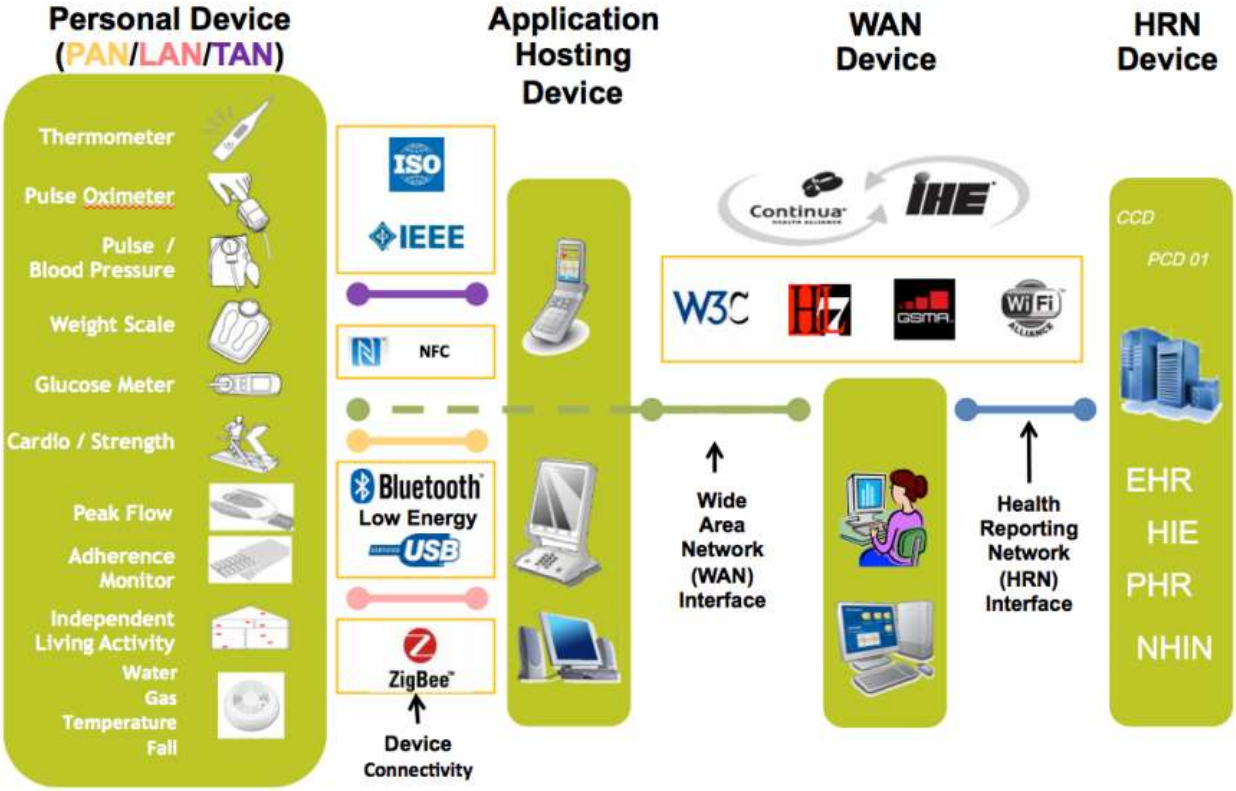
[79] http://www.mhealthsummit.org/
[80] http://www.himss.org/
[81] http://www.pchalliance.org/
[82] http://www.continua.jp/docs/20140422_PCHA_Launch_Press_Release_FINAL_JPN_FIN02.pdf
[83] http://www.continua.jp/docs/20140422_PCHA_Launch_Press_Release_FINAL_JPN_FIN02.pdf
[84] http://www.pchalliance.org/pcha-leadership-and-board
[85] http://www.continuaalliance.org/node/78
[86] https://allseenalliance.org/announcement/personal-connected-health-alliance-and-allseen-alliance-forge-iot-healthcare

この Continua Design Guidelines は、PCHA または Continua Health Alliance のメンバーであれば無料でダウンロードできるようになっている。該当のウェブページ[87]からも確認できるように、毎年新しいバージョンのガイドラインが公開されている。

なお、同ガイドラインは 2013 年 12 月 19 日には ITU により ITU-T H.810 としても採用されている[88]。ITU-T が 2014 年 7 月に発行したテクニカルペーパー[89]でも、現在の Continua Design Guidelines が採用しているアーキテクチャが示されている。

以下の図表 20 は、ITU-T が紹介する Continua Design Guidelines のアーキテクチャを示したものである。ここからわかるように、機器同士の通信には IEEE 11073 の標準規格が採用されている。また、医療情報を表現し交換するための規格としては HL7 が、この HL7 の使い方を表現する規約[90]としては IHE が採用されている。

図表 20：ITU-T が紹介する Continua Design Guidelines のアーキテクチャ



出典：ITU-T[91]

Continua Design Guidelines の異分野の IoT 基盤との連携については、公開されている情報では確認できなかった。

[87] http://www.continuaalliance.org/products/design-guidelines
[88] https://www.itu.int/net/pressoffice/press_releases/2013/75.aspx
[89] https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-EHT-2014-H810-PDF-E.pdf
[90] http://www.innervision.co.jp/12SP/ihefaq/vol1.html
[91] https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-EHT-2014-H810-PDF-E.pdf

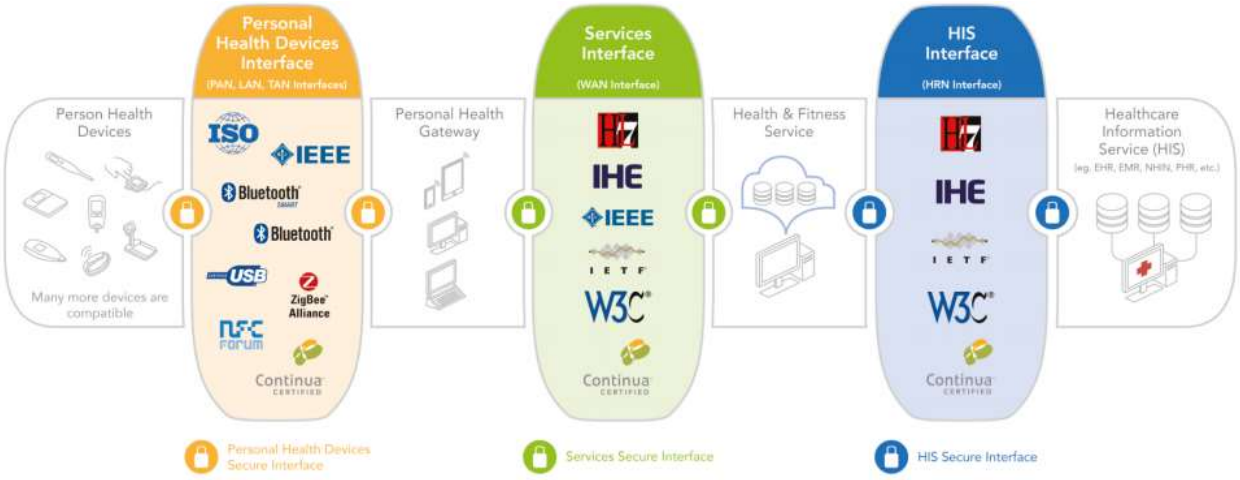
d. Continua Design Guidelines のテストベッド

上記の通り、PCHA または Continua Health Alliance のメンバーは Continua Design Guidelines を無料でダウンロードできる他、CESL（Continua Enabling Software Library）と呼ばれるライブラリやテストツールについても入手することができる[92]。メンバーはまた、製品の市場投入前に相互接続性テストなどを行うことも可能となっているが、詳細については確認できなかった。

e. Continua Design Guidelines のセキュリティ

以下の図表 21 は PCHA 自身が公開しているホワイトペーパー内で示されている Continua Design Guidelines のアーキテクチャである（上記の図表 20 は ITU-T によって示された Continua Design Guidelines のアーキテクチャ）。ヘルスケア機器（図の一番左側）からゲートウェイに至るまでの Personal Health Devices Interface（図中オレンジの部分）、そこからヘルスケア関連のサービスに至るまでの Services Interface（図中緑の部分）、更にそこからヘルスケア情報サービスに至るまでの HIS Interface（図中青の部分）が示されている。

図表 21：PCHA による Continua のアーキテクチャ



出典：PCHA[93]

Continua Design Guideline では、この 3 種類のインターフェースそれぞれで、アイデンティティマネジメント、同意のマネジメント、認証などによりセキュリティとプライバシーの課題に対応しているとしている。

（7） 社会インフラ分野の IoT 基盤：OpenFMB

a. OpenFMB の概要

OpenFMB（Open Field Messaging Bus）とは、NIST の元でスマートグリッド関連の標準化策定に取り組んでいた SGIP（Smart Grid Interoperability Panel）による EnergyIoT（エネルギー分野の IoT）プロジェクトで提示されているフレームワークである[94]。具体的には、点在する分散電源などに関する情報を収集しやすくするための仕組みとして機能するものと言える。分散電源とは、太陽光発電や風力発電などの再生可能エネルギーや蓄電池などの、電力事業者側で集中的に管理できない、利用者の近くに点在しているような要素を総称したものである。SGIP のウェブサイトでは ”distributed intelligent nodes” と「ノード」という表現がされている[95]。

[92] http://www.continuaalliance.org/products/design-guidelines
[93] https://cw.continuaalliance.org/document/dl/13473
[94] http://sgip.org/Open-Field-Message-Bus-OpenFMB-Project
[95] http://sgip.org/Open-Field-Message-Bus-OpenFMB-Project

電力業界では現在、太陽光発電などの導入が増えることに伴い、ある一定の需要地内で複数の自然変動電源や制御可能電源を組み合わせて制御し、電力・熱の安定供給を可能とする小規模な供給網（マイクログリッド）[96]の導入が増えていくことが予想されている。そうした中、再生可能エネルギー関連の機器や蓄電池などのメーカーが異なることを理由に、それらの情報を一括して管理することができないという課題が生じていたため、これを解決するためのソリューションフレームワークとして、メーカーが異なる機器同士であっても発電量や消費量に関するデータをやり取りし、統合的な管理を実現できる OpenFMB が開発されているわけである。

b. SGIP の活動概要

OpenFMB フレームワークの開発は、Green Button の項目でも紹介した SGIP（Smart Grid Interoperability Panel）において進められている。上記でも紹介したように、SGIP はスマートグリッドの標準化活動を進めるため、2009 年 11 月に NIST が主導する形で組織化した団体である。当時の SGIP の目的は、スマートグリッドにかかわる多数のステークホルダーを調整し、標準化策定の取り組みを推進することであったが、その後、当初の目的は果たしたとして、NIST 主導ではなく官民一体でスマートグリッドを主導すべく、新たに非営利団体としての SGIP が組織化されている。業界では、この新生 SGIP をこれまでの SGIP と区別して SGIP 2.0 と呼ぶ場合もある[97]。

SGIP 2.0 の 2016 年のボードメンバーには、Electric Reliability Council of Texas、EnerNex LLC、NEMA（National Electrical Manufacturers Association）などが名を連ねている。その他のメンバーを見ても、営利企業よりは政府系の組織や研究所の出身者が多くの数を占めているといった特徴がある[98]。

OpenFMB フレームワークの開発に向けた動きは、この SGIP において 2015 年に開始されたプロジェクトという位置づけにある。プロジェクトはノースカロライナ州の大手電力事業者である Duke Energy 社が中心となって進めているが、他の電力事業者、研究開発組織、標準化団体なども開発に参画している。営利企業としては ABB 社、Aclara 社、Ericsson 社、GE 社、Green Energy 社、伊藤忠、Itron 社、Kitu Systems 社、LocalGrid 社、OMNETRIC 社、RTI 社、ViaSat 社などが開発参画企業として名を連ねている[99]。

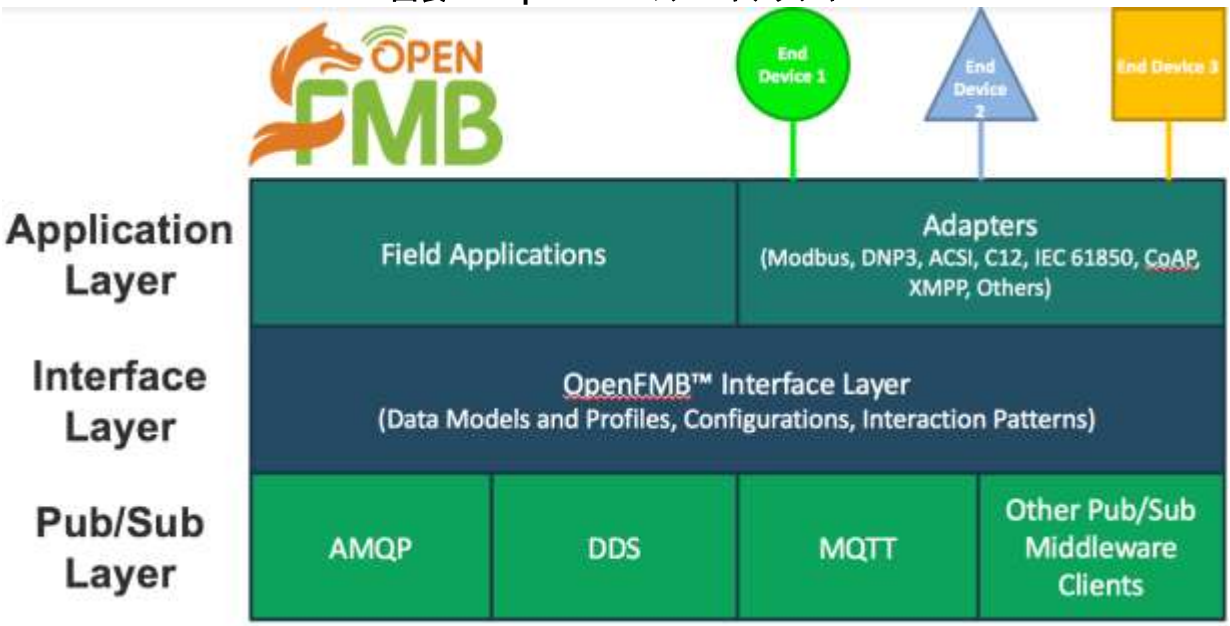
c. OpenFMB の機能

OpenFMB フレームワークは、Modbus や DNP3、IEC 61850 など、さまざまな標準規格を採用したアプリケーションに対応したアーキテクチャフレームワークとなっている。このアーキテクチャを採用すると、電力事業者などは、それぞれの分散電源が採用している技術の違いなどを意識することなく、分散電源を柔軟に管理できるようになる点が特徴である。

以下の図表 22 は、OpenFMB フレームワークを開発する際のアーキテクチャを示したものである。どのようなアプリケーションからのデータであっても OpenFMB がインターフェースとなってやり取りをすることで互換性を担保する形となっている。最下層にはパブリッシュ/サブスクライブ型のレイヤがあり、MQTT や DDS などのプロトコルが対応している。

[96] http://www.nedo.go.jp/content/100083461.pdf
[97] http://sgip.org/SGIP-History
[98] http://sgip.org/Board-of-Directors
[99] http://www.sgip.org/OpenFMB-Team

図表 22：OpenFMB のアーキテクチャ



出典：SGIP[100]

なお、OpenFMB フレームワークの異分野の IoT 基盤との連携についての情報は確認できなかった。現時点では、OpenFMB はまだデモンストレーションを繰り返すといった実証段階にあるためのため、異分野の IoT 基盤との連携については、検討されるにしてもまだ先になると見られる。

d. OpenFMB のテストベッド

OpenFMB フレームワーク開発プロジェクトのメンバー専用ウェブページ[101]を見ると、テストベッドを提供しているメンバーが確認できる。具体的には、同プロジェクトを牽引するノースカロライナ州の Duke Energy 社の他、テキサス州の電力事業者である CPS Energy 社、そして NREL（米国国立再生可能エネルギー研究所）という 3 組織の名前があがっている。

なお、SGIP は現在、これらのテストベッドなど利用して OpenFMB フレームワーク開発プロジェクトでの取り組み成果を積極的にデモンストレーションしている。直近では、2016 年 2 月にフロリダ州で開催されたエネルギー関連のイベントである DistribuTECH[102]でも、テストベッドを利用した取り組みのデモンストレーションが行われた。

e. OpenFMB のセキュリティ

OpenFMB フレームワーク開発プロジェクトの概要を示したプレゼンテーション資料[103]によると、OpenFMB のセキュリティはネットワーク部分でセキュリティ対策を施している他、データを管理するホスト部分でもセキュリティ対策をしている。これは、DDS などのプロトコル自体が持つセキュリティ機能などを組み合わせて実現しているという。

[100] http://www.sgip.org/SGIP/files/ccLibraryFiles/Filename/000000001879/SGIP Open Field Message (OpenFMB) Bus Project V1.8.pptx
[101] http://www.sgip.org/OpenFMB-Team
[102] http://www.distributech.com/index.html
[103] http://www.sgip.org/SGIP/files/ccLibraryFiles/Filename/000000001879/SGIP Open Field Message (OpenFMB) Bus Project V1.8.pptx

（8） 分野横断型の IoT 基盤①：oneM2M

a. oneM2M の概要

oneM2M とは、M2M に関する標準規格が乱立することを避けるため、世界各国の電気通信系の標準化団体が協力しながら策定検討する M2M/IoT の共通基盤のことである。グローバルに通用する M2M/IoT 仕様の確立を目的として、サービス層のプラットフォームにフォーカスして共通仕様の定義が進められている。oneM2M にかかるサービス層のプラットフォームには、オープンなインターフェースやプロトコルのほか、相互運用性やテストなどの仕様までも含まれている[104]。同プラットフォームを策定するのも、oneM2M という団体となっている。

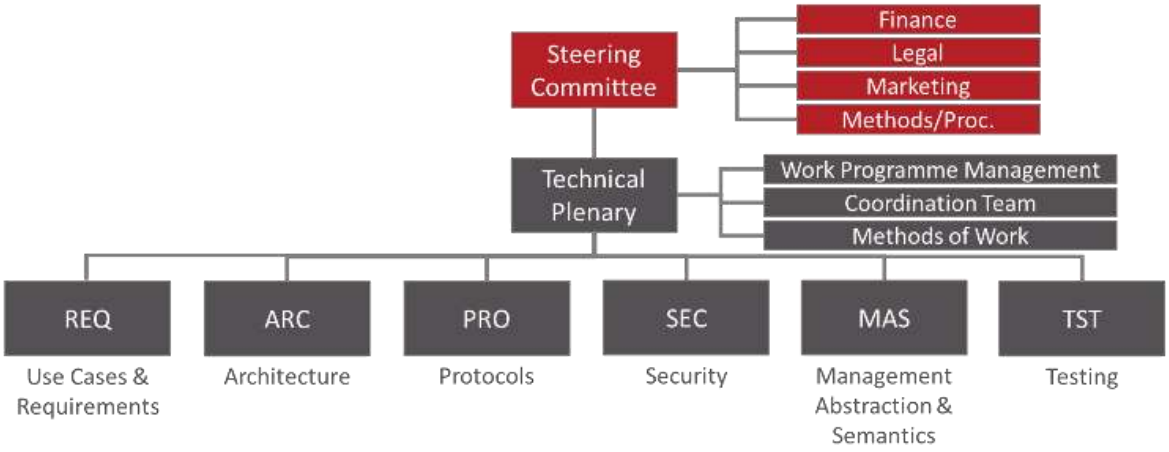
b. oneM2M の活動概要

団体としての oneM2M の設立のきっかけは、2009 年 1 月の欧州の電気通信関連の標準化団体 ETSI 内に M2M アーキテクチャなどを検討する TC M2M が設置されたことに遡る。しかし、この ETSI による TC M2M の設置以降、国際的にさまざまな標準化団体が M2M に関する標準化に乗り出し、さまざまな M2M 関連の規格が乱立する恐れが出てきたため、まずは 2011 年 7 月に ETSI の提唱により、各国の標準化団体が協力する形で共通の M2M 関連規格を策定するという非公式な委員会が設立された。

oneM2M は、この非公式な委員会をもとに 2012 年 7 月に正式な団体として設立されたことで誕生した。中心メンバーは基本的に M2M にかかる標準化団体であり、設立当時は日本の ARIB と TTC、米国の ATIS と TIA、中国の CCSA、欧州 ETSI、韓国 TTA であったが、現在はこれにインドの TSDSI も加わっている[105]。現在は 228 の団体や企業が oneM2M に加盟している[106]。

現在の組織体制[107]であるが、主に運営面の活動を担う Steering Committee と技術面の活動を担う Technical Plenary で構成されており、その下で REQ（ユースケースと要件）、ARC（アーキテクチャ）、PRO（プロトコル）、SEC（セキュリティ）、MAS（管理、抽象化、セマンティックス）、TST（テスト）という 6 つのワーキンググループが活動している。以下の図表 23 は oneM2M の組織体制を示したものである。

図表 23：oneM2M の組織体制



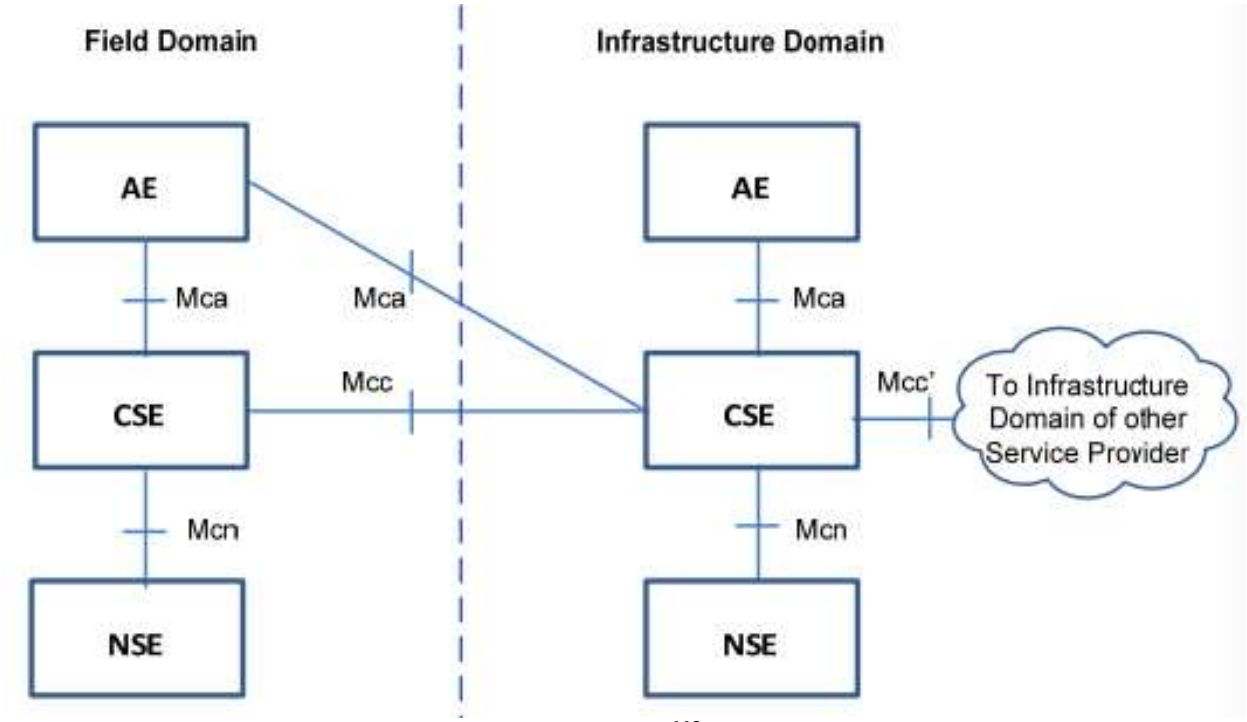
出典：oneM2M[108]

[104] http://www.slideshare.net/onem2m/iot-service-layer-evolution?ref=http://www.slideshare.net/onem2m/slideshelf
[105] http://monoist.atmarkit.co.jp/mn/articles/1511/19/news018.html
[106] http://www.onem2m.org/membership/current-members
[107] http://www.onem2m.org/about-onem2m/organisation-and-structure
[108] http://www.onem2m.org/about-onem2m/organisation-and-structure

c. oneM2M の機能

oneM2M は 2012 年 7 月設立であり、今回取り上げる団体の中で最も古い歴史をもつが、技術仕様のリリース 1 が発表されたのは 2015 年 1 月と比較的最近である。そのアーキテクチャは、アプリケーション・エンティティ（AE）、共通サービス・エンティティ（CSE）、ネットワークサービス・エンティティ（NSE）で構成されるものとなっており、このうち CSE が oneM2M の標準化の取り組みの中心となっている[109]。以下の図表 24 は、リリース 1 で示された oneM2M のアーキテクチャを示している。

図表 24：oneM2M のアーキテクチャ



出典：TTC[110]

なお、oneM2M の中核である CSE では、次に示す 12 種類の共通サービス機能が定義されている。

- アプリケーション及びサービス層管理
- 通信管理・配布管理
- データ管理・蓄積
- デバイス管理
- 検出
- グループ管理
- 位置情報
- ネットワークサービス連携
- 登録
- セキュリティ
- サービス課金・管理
- サブスクリプション・通知

[109] http://www.ttc.or.jp/jp/document_list/pdf/j/TR/TR-M2M-R1v1.0.0.pdf
[110] http://www.ttc.or.jp/jp/document_list/pdf/j/TR/TR-M2M-R1v1.0.0.pdf

oneM2M の異分野の IoT 基盤との連携であるが、oneM2M 自体がさまざまな標準化団体が集まる形で策定された仕様であり、分野横断型の仕組みとなっている。また、その設立および仕様策定の経緯もあり、将来的に他の IoT 基盤との連携が模索される可能性も十分にある。

d. oneM2M のテストベッド

oneM2M は上記の技術仕様のリリース 1 を発表した後の 2015 年 9 月 14 日～16 日に、仕様に準じて開発された機器同士の相互接続試験を実施している[111]。また、2016 年 2 月 4 日に 2 回目の相互接続試験を実施する予定があることも発表している[112]。

e. oneM2M のセキュリティ

oneM2M の技術仕様リリース 1 では、文書番号 TS-M2M-0003v1.0.1 においてセキュリティ技術の適用が言及されている[113]。この中で、oneM2M が想定しているセキュリティ機能として、認証、承認、アイデンティティ管理、センシティブなデータの扱い、セキュリティ管理などがあげられている。

（9） 分野横断型の IoT 基盤②：AllJoyn

a. AllJoyn の概要

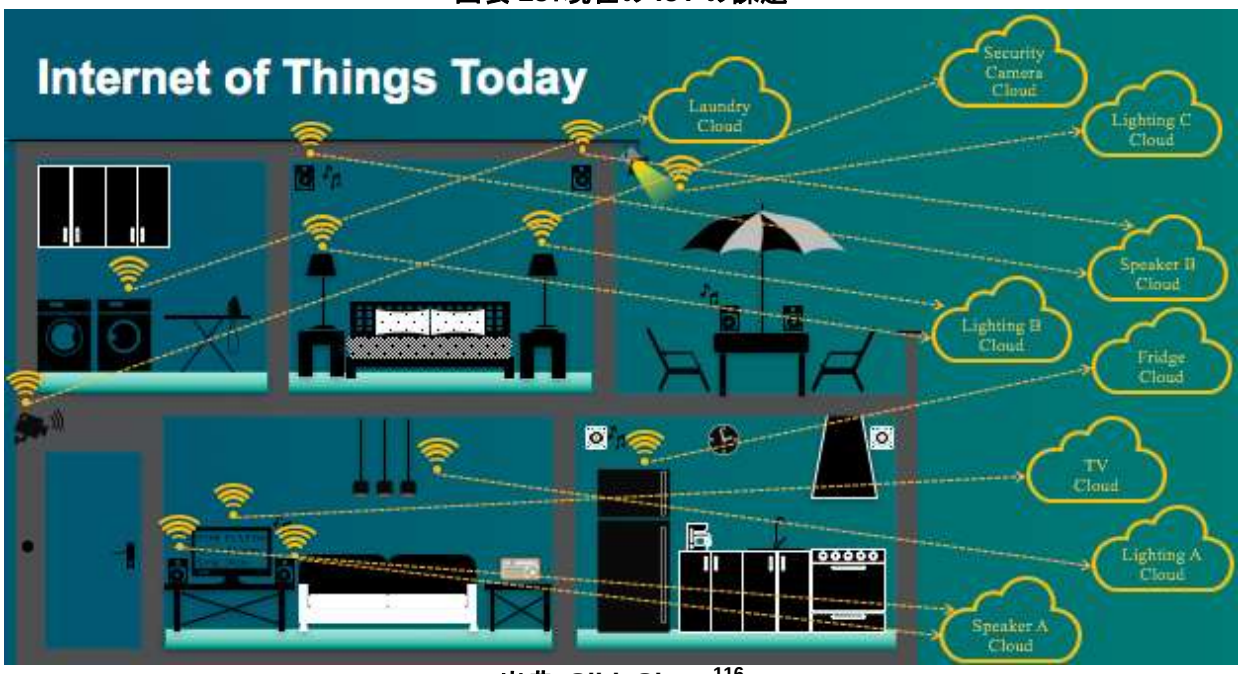
AllJoyn とは、IoT にかかるさまざまなデバイスやアプリケーションが機器、ブランド、分野、OS といった違いに関係なく相互接続性を担保できるようにすることを目的に、Linux Foundation のコラボラティブプロジェクト AllSeen Alliance[114]が開発するオープンソースベースのフレームワークである。もともとは Qualcomm 社の Qualcomm Innovation Center が独自に取り組んでいたオープンソースプロジェクトであったが、企業・業界横断的な取り組みにするために Linux Foundation に移管され、現在では Linux Foundation におけるコラボラティブプロジェクト AllSeen Alliance が策定するフレームワークという位置づけにある。

AllSeen Alliance は、現在の IoT 環境が個々のデバイスやアプリケーションがそれぞれ対応するソフトウェアとやり取りをしているだけであり、相互に連携する状況にないという問題意識のもと、AllJoyn フレームワークの開発を進めている。デバイスやアプリケーションが API を提供しているような場合でも、個々のデバイスやアプリケーションによって使われている API 仕様が異なるケースがほとんどであるため、API が提供されていても相互互換性などは実現していないとした上で、この課題を解決するためのフレームワークとして AllJoyn が提唱されている[115]。

以下の図表 25 は、AllSeen Alliance が指摘する現在の IoT 環境の問題を示したものである。冒頭で紹介したサイロ型の問題と同じ環境が示されている。

[111] http://www.onem2m.org/news-events/news/86-multi-vendor-interoperability-event-validates-onem2m-standard-for-iot
[112] http://www.onem2m.org/news-events/news/95-onem2m-to-host-second-interoperability-event
[113] http://www.ttc.or.jp/jp/document_list/pdf/j/TS/TS-M2M-0003v1.0.1.pdf
[114] https://allseenalliance.org/
[115] http://www.slideshare.net/AllSeenAlliance/programming-the-internet-of-things-why-devices-need-apis

図表 25：現在の IoT の課題



出典：SlideShare[116]

b. AllSeen Alliance の活動概要

AllSeen Alliance が開発している AllJoyn は上記の通り、もともとは Qualcomm Innovation Center が独自のオープンソースプロジェクトとして開発する仕様であった。その後、この開発プロジェクトの管理をオープンソース団体である Linux Foundation[117]に譲渡したが、2014 年 12 月には Linux Foundation が主導となって AllSeen Alliance が設立された。

AllSeen Alliance の設立メンバーは Haier 社、LG Electronics 社、パナソニック、Qualcomm 社、シャープ、Silicon Image 社、TP-LINK 社の 7 社であったが、現在は数多くの企業が参加しており、業界をリードする企業によるコラボラティブなプロジェクトという位置づけにある。

c. AllJoyn の機能

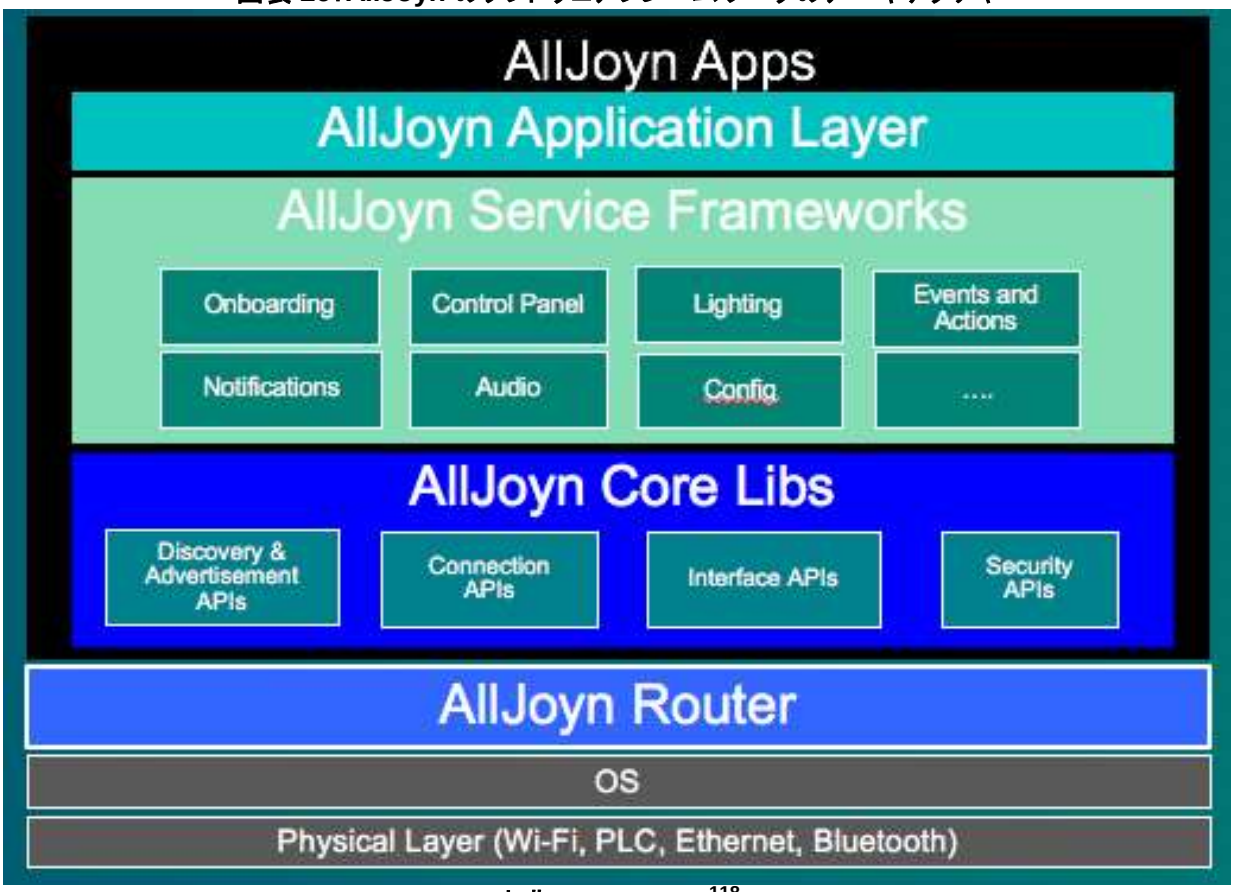
AllJoyn で定義されるアーキテクチャは、①AllJoyn アプリケーション層、②AllJoyn サービスフレームワーク、③AllJoyn コアライブラリ、という三層構造になっており、さらにその下に AllJoyn ルーターが位置づけられている。それぞれの概要は以下の通りである。

① AllJoyn アプリケーション層：ユーザエクスペリエンスを定義している。
② AllJoyn サービスフレームワーク：プラットフォーム間での相互接続性を担保するために、デバイス間の共通インターフェースを定義している。
③ AllJoyn コアライブラリ：デバイスの検出と接続といった機能、アクセスコントロールや暗号化といった機能を提供している。

以下の図表 26 は、AllJoyn のソフトウェアフレームワークのアーキテクチャを示したものである。三層のライブラリはいずれも、その下に位置する AllJoyn ルーターとやり取りをする仕組みとなっている。

[116] http://www.slideshare.net/AllSeenAlliance/programming-the-internet-of-things-why-devices-need-apis
[117] http://collabprojects.linuxfoundation.org/

図表 26：AllJoyn のソフトウェアフレームワークのアーキテクチャ



出典：SlideShare[118]

AllSeen Alliance に参加するメンバー企業各社は、この AllJoyn フレームワークを活用して製品開発を行っている。AllSeen Alliance は認証プログラムも提供しており、AllSeen Alliance の認証を受けた製品リストには、既に 23 の製品が掲載されている[119]。

異分野の IoT 基盤との連携であるが、oneM2M 同様に分野横断型の仕組みとなっており、複数分野をカバーしている。なお、後ほど OCF の部分でも紹介する通り、AllSeen Alliance を主導する代表メンバーの Qualcomm 社、Microsoft 社などは近、同じく分野横断的な IoT 向け標準仕様を策定する OIC（Open Interconnect Consortium）の後継団体 OCF（Open Connectivity Foundation）にも参加しており、両団体が連携して IoT 向けの単一のオープンな標準仕様の確立に向けて動きだすことを期待する声は大きい。

d. AllJoyn のテストベッド

AllJoyn は上記の通り認証プログラムを提供しており[120]、各製品が AllJoyn のインターフェース定義に適合しているかどうかを確認した上で認証している。AllJoyn 認証製品間では相互接続性が確認された形となる。AllSeen Alliance はこの認証プログラムにおいて、一般に対して認証テストツールを提供している。なお、この AllJoyn 準拠認証については、AllSeen Alliance のメンバー以外も受けることができ、認証されるためにメンバーになる必要はない。

[118] http://www.slideshare.net/AllSeenAlliance/programming-the-internet-of-things-why-devices-need-apis
[119] https://certify.alljoyn.org/certified-products
[120] https://certify.alljoyn.org/docs/certification-guide

e. AllJoyn のセキュリティ

AllJoyn フレームワークでは、アプリケーションレベルでのセキュリティを提供している。具体的には、認証とデータの暗号化がアプリケーションレベルで行われる形となっている[121]。

（10）分野横断型の IoT 基盤③：IoTivity

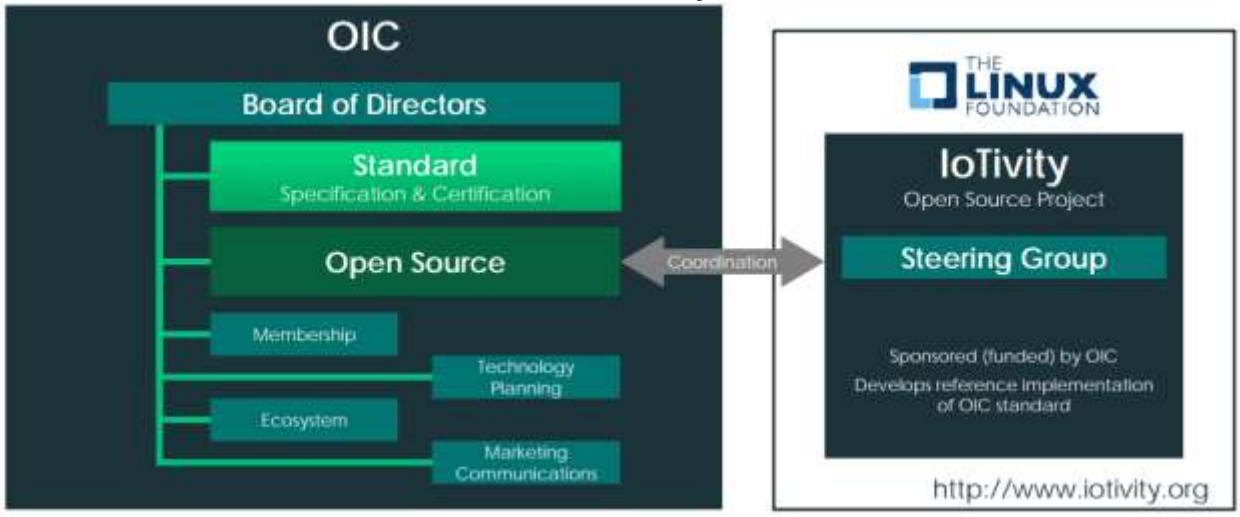
a. IoTivity の概要

IoTivity[122]とは、IoT 向けの標準仕様を策定する業界団体 OCF (Open Connectivity Foundation)によるオープンソースなソフトウェアフレームワークである。OCF はネットワークに接続されるあらゆるデバイスがメーカーや OS、チップセットなどの違いに限らずにお互いに通信できるようになるべきであるとの考えのもと、それを実現するために IoTivity をオープンソースベースのソフトウェア仕様として策定し、オープンソースプロジェクトとして展開している[123]。

IoTivity はあらゆるデバイスを相互に接続する目的で定義されたソフトウェアフレームワークであると同時に、サービスの開発を加速するために作られたオープンソースコミュニティでもある。OCF が主導しているが、AllJoyn の開発を主導する AllSeen Alliance と同様に、Linux Foundation におけるコラボラティブプロジェクトという位置づけにもある。

以下の図表 27 は OCF（前 OIC：Open Interconnect Consortium）と IoTivity プロジェクトの関係性を示したものである。詳細は以下に譲るが、OCF は OIC の後継組織として設立された業界団体であり、現時点で OCF が提供する情報には OIC 時代のままのものが多い。

図表 27：OIC（現 OCF）と IoTivity プロジェクトの関係



出典：OCF[124]

b. OCF の活動概要

OCF は上記の通り、OIC の後継組織として設立された業界団体である。OIC はもともと、2014 年 7 月に Intel 社が主導する形で Atmel 社、Broadcom 社（その後退会）、Dell 社、Samsung 社、Wind River 社をあわせた計 6 社で誕生した。その後 2015 年 11 月には、IoT 向けの独自仕様の策定に動いていた UPnP

[121] https://allseenalliance.org/framework/documentation/learn/core/system-description/alljoyn-security
[122] https://www.iotivity.org/about
[123] http://openconnectivity.org/
[124] http://openconnectivity.org/wp-content/uploads/2016/01/OIC_Specification_Overview_201501131.pdf

Forum（Universal Plug and Play）を完全に吸収しており[125]、UPnP Forum の加盟企業までをメンバーとして迎えており（1,000 社を超える UPnP の会員のうち会費を支払っていない基本レベルのメンバー約 840 社は対象外）[126]、大規模な組織となった。

更に、2016 年 2 月 19 日には OIC は新たな組織 OCF となることを発表し、現在では OCF として活動を行っている。この OCF となった際に注目されたのが、対立するとされてきた AllJoyn フレームワークを策定する AllSeen Alliance の主要メンバーである Qualcomm 社、Microsoft 社、Electrolux 社の 3 社が OCF に参加したことである[127]。OIC 時代の UPnP Forum 吸収時には、「OIC は UPnP Forum ではなく AllSeen Alliance と歩調をそろえて、プロプライエタリな規格を推進する Google 社や Apple 社に立ち向かうべきだ」とする声が専門家の間で出ていたが、一方で OIC が UPnP Forum を吸収したことで、UPnP 仕様で策定されているサービス検出手法を採用することが決定的になり、更なる団体との連携は難しいのではないかという指摘も出ていた[128]。

そうした中で、AllSeen Alliance の主要メンバーである Qualcomm 社、Microsoft 社、Electrolux 社が OCF に参加したため、AllSeen Alliance と OCF は正式に連携または合併するのではないかとする声も出ていたが、Qualcomm 社の Senior Vice President である Michael Wallace 氏は OCF 発足翌日のブログにおいて、団体の統合までは行わない旨のコメントを出している。以下は、同氏がブログに投稿した「断片化は IoT の敵」というタイトルの記事における、同氏のコメントである[129]。

> 「Qualcomm 社は今後とも AllSeen Alliance のメンバーであり、単一のオープンな IoT 標準の確立を手助けすべく、双方の組織に協力していく。私たちは製品・サービス間の接続およびやり取りに関するオープンで強力な標準を信条としており、本当に単一の IoT 標準が実現すれば、目的を達成したといえるようになるだろう[130]」。

Wallace 氏の上記のコメントからもわかるように、AllSeen Alliance と OCF が合併するのではないかという声は今もあるが、両団体は合併統合するのではなく、複数の IoT 標準規格の乱立を回避するために協業をしていくというスタンスにあると考えられる。

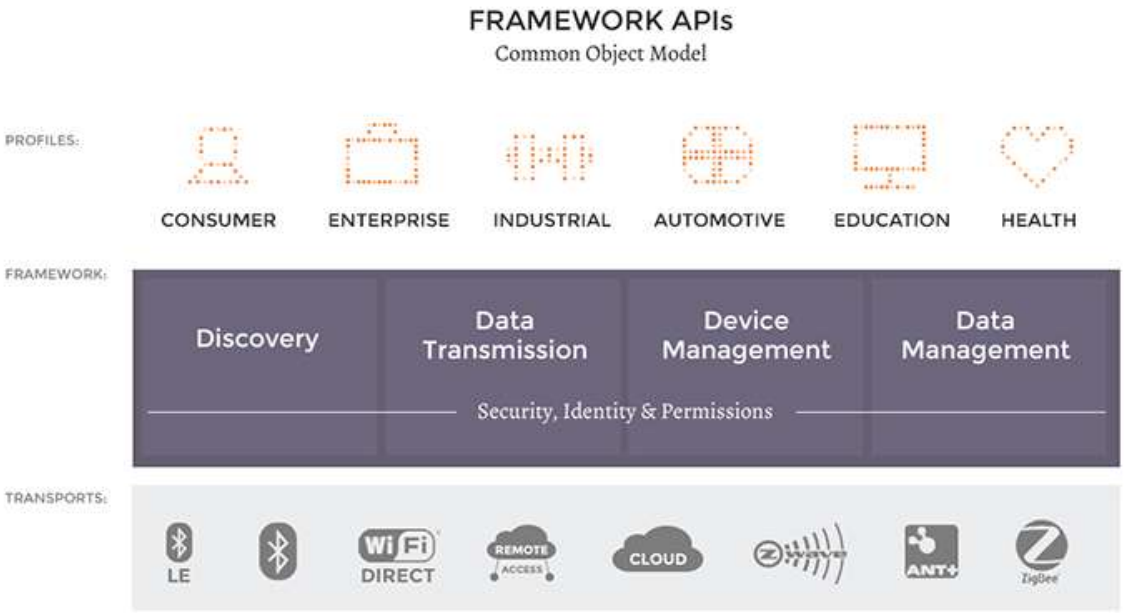
c. IoTivity の機能

IoTivity とは上記の通り、OCF による支援のもと Linux Foundation におけるコラボラティブプロジェクトで開発されている IoT 向けのオープンなソフトウェアフレームワークである。IoTivity フレームワークは、IoT のトランスポートレイヤ（通信ネットワーク）とプロファイルレイヤ（IoT サービス向けユーザプロファイル）の中間に位置するものとなっており、「Discovery（デバイスなどの検出）」、「Data Transmission（データ転送）」、「Device Management（デバイス管理）」、「Data Management（データ管理）」という 4 つの主要機能が用意されている。いずれにおいても複数のプログラミング言語や OS に対応した API が用意され、開発者向けに提供される予定となっている。

以下の図表 28 は、IoTivity フレームワークを示したものである。図の中央のフレームワークレイヤが IoTivity であり、その下のトランスポートレイヤにあるさまざまな通信規格やプロファイルレイヤにある様々な IoT サービスプロファイルに対応しながら、ミドルウェアのような働きをするものと位置づけられている。

[125] http://www.businesswire.com/news/home/20151125005936/ja/
[126] http://eetimes.jp/ee/articles/1511/26/news053.html
[127] http://openconnectivity.org/news/open-connectivity-foundation-brings-massive-scale-to-iot-ecosystem
[128] http://eetimes.jp/ee/articles/1511/26/news053.html
[129] https://www.qualcomm.com/news/ong/2016/02/19/fragmentation-enemy-internet-things
[130] http://www.atmarkit.co.jp/ait/articles/1602/22/news054.html

図表 28：IoTivity フレームワーク



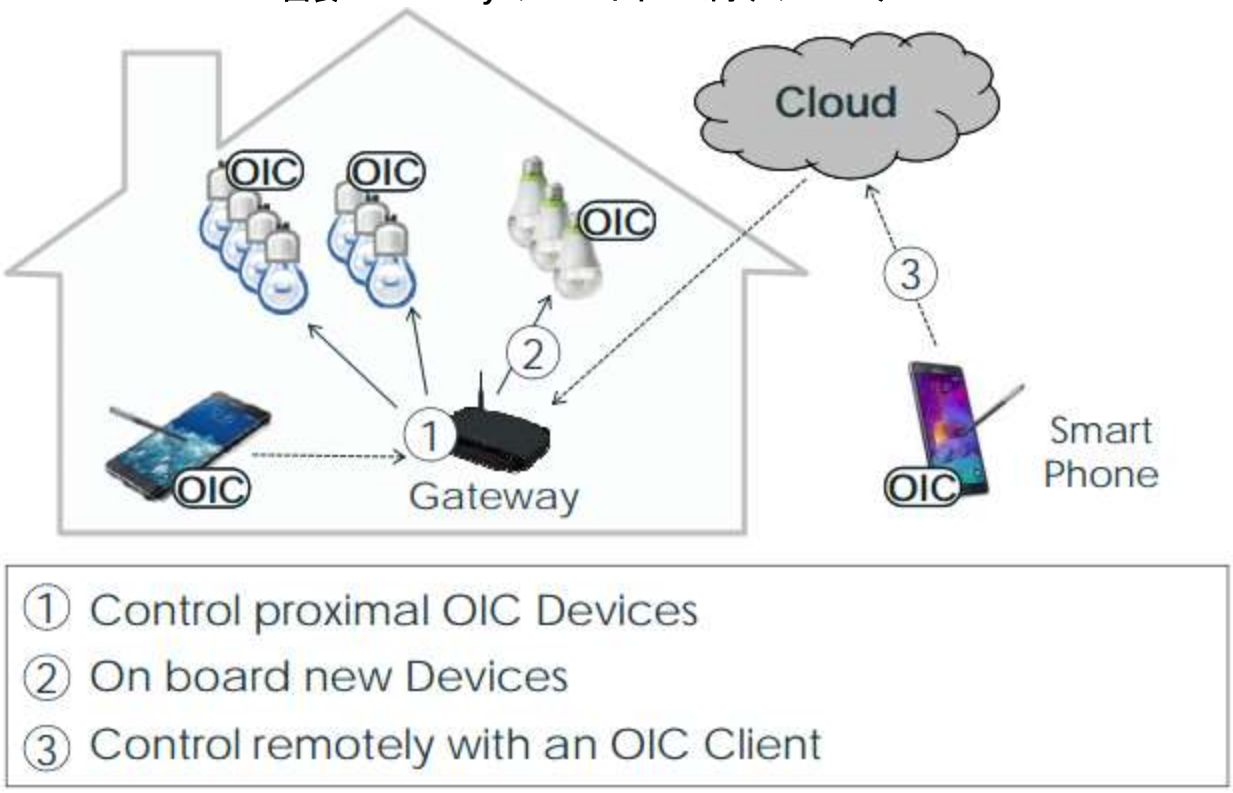
出典：IoTivity[131]

なお、IoTivity フレームワークのリリース 1.0.0 の機能一覧を確認すると[132]、同フレームワークには Smart Home Protocol Control Manager という機能が提供されたことがわかる。上記の図表 28 の最上部にあるプロファイルレイヤでは、消費者向け、企業向け、産業向け、車向け、教育向け、ヘルスケア向けなどのユーザプロファイルが想定されているが、IoTivity 1.0.0 に含まれた Smart Home Protocol Control Manager はその中でも消費者向けのプロファイルに対応し、スマートホーム向けの IoT プロトコルを制御するものとなっていると言える。

なお、OIC が OCF として生まれ変わる直前の 2016 年 1 月に OIC により公開された IoT 標準仕様の紹介資料[133]の後半では、このスマートホーム向けの IoTivity フレームワークのユースケースが紹介されている。これを抜粋したものが以下の図表 29 であり、ここでは IoTivity フレーワークに対応した IoT 機器が OIC として表現されている。このユースケースでは、①近くにある IoT デバイス（OIC）を制御する場合、②IoT デバイス（OIC）に組み込む場合、③IoT デバイス（OIC）を遠隔で制御する場合、の 3 パターンをもってスマートホームのユースケースを検討している。

[131] http://openconnectivity.org/wp-content/uploads/2016/01/OIC_Specification_Overview_201501131.pdf
[132] https://www.iotivity.org/documentation/features
[133] http://openconnectivity.org/wp-content/uploads/2016/01/OIC_Specification_Overview_201501131.pdf

図表 29: IoTivity のスマートホーム向けのユースケース



出典:OIC[134]

d. IoTivity のテストベッド

IoTivity プロジェクトではテストベッドの存在を確認できなかったが、OCF としては認証プログラムを提供する予定となっている。ただし、現時点ではプログラム自体を開発中であり、認証プログラムはまだ機能していない[135]。なお、OCF の認証プログラムに関する詳細情報は OCF のメンバー専用ページで公開されていないため、一般からはどういったプログラムになるかは確認できない状況にある。最終的にどういったプログラムが誰に展開されるかは定かではないが、認証対象がメンバーに限定される場合は、誰でもが認証プログラムを受けることができる AllSeen Alliance との大きな差になると言える。

e. IoTivity のセキュリティ

IoTivity フレームワークでは、上記の図表 28 を見てもわかるように、セキュリティ、アイデンティティ、パーミッションなどをカバーしている。これらのセキュリティ機能に関しても、このフレームワークレイヤで対応する予定となっている。

[134] http://openconnectivity.org/wp-content/uploads/2016/01/OIC_Specification_Overview_201501131.pdf
[135] http://openconnectivity.org/certification

4　終わりに

上記で見てきたように、大きく成長する可能性を秘めた IoT 市場では、さまざまな業界団体が IoT 基盤の開発および普及に向けて積極的に取り組んでいる。また、そうした動きを加速させようと、IIC と Industrie 4.0 との協業、Continua Health Alliance と他団体が合併する形での Personal Connected Health Alliance の設立、そして、非公式ではあるものの主要メンバーを通した AllSeen Alliance と OCF の協業など、団体間での連携の動きも出てきている。このような統合や協業の動きは、多くのステークホルダーを取り込み、それぞれの標準規格やフレームワークの採用を後押しすることになる重要な動きと言える。

一方で、本レポートでは取り上げなかった Apple 社や Google 社などの個別企業が策定・提供する IoT 基盤をめぐる動きには引き続き注視していかなければならない。特にこの両社は、市場に多く出回っている iOS 端末と Android 端末などを入口としてユーザに入り込みやすい環境を整えている。いずれも自社 OS を軸に IoT 市場のデファクトスタンダードをとっていくことを狙っており、標準化団体が IoT 仕様をもとにユニバーサルな環境を普及させようとしても、こうした単独企業の動きが障害になる可能性は否定出来ない。

IoT ビジネスで競合企業に先んじるためには、なによりも早い段階で製品やサービスを市場に投入することが重要になってくる。しかし、そのタイミングでは、まだどの IoT 基盤が市場で優位性をもつのかが定まっていない可能性が高い。今後、日本の IoT 企業が IoT ビジネスを進めていく上では、市場動向と合わせて、IoT 基盤も含めた技術動向にも注意を払いながら、サービス開発を進めていくことが重要となってくると考えられる。