研　究　解　説

相互接続基盤としてのIoT-HUBの活用方策

Study of challenges and solutions on IoT-HUB for practical use as an interconnection infrastructure

馬　場　博　幸*・野　城　智　也*
Hiroyuki BABA and Tomonari YASHIRO

要　　旨

IoTは個別のシステムを相互に接続することにより極めて多様な価値を生み出す可能があると期待されている．しかしながら，通信プロトコルの整合性や障害発生時の対応方策，更にはビジネス上の懸念点などがあり，自在な相互接続を実現するにはこれらの問題点を解決する必要があった．筆者らは産学連携活動によって開発したIoT-HUBと呼ぶ相互接続インフラを基盤にこれらの解決策を考案し，その活用方策について検討したので，考案内容，検討内容について報告する．

Abstract

In IoT field, generation of huge various value by interconnection of individual IoT systems is expected. However consistency of communication protocol, countermeasures against service trouble, concerns as business scheme and so on must be solved to realize interconnection of IoT-systems. This paper reports challenges and solutions on the IoT-HUB, interconnection infrastructure for IoT, which is developed industry-academia collaboration at Institute of Industrial Science, The University of Tokyo.

1．は　じ　め　に

筆者らはデジタルトランスフォーメーション（DX）の重要な要素となるIoT（Internet of Things）に注目し，産学連携の許，課題整理とその解決策について生産技術研究所内の実験ハウス（通称：COMMAハウス，図1）にて様々な試験実装等を続けて来た．その結果，異なるConnectedな機器やアプリ（以下，IoTシステム）を相互に接続するIoT-HUBと呼ぶインフラの開発に至り，産学連携先によってそれが社会実装されて，現在実際のユーザーに使用され始めている．実ユーザーに使用されるには技術問題だけではなくビジネス上の問題も解消する必要があり，本稿はそれらへの対応を纏めた報告である．

図1　COMMAハウス

*東京大学生産技術研究所　人間・社会系部門

2．IoTの課題

IoTは，あらゆるものがネット（一般的にはインターネット）に繋るという概念である．ネットを単に通信用パイプとして捉え，センサーやスマートフォンアプリなど自社の製品群から成るクローズドなシステムを構築する方法もあるが，あらゆるものがネットに繋がるのであれば，他社の製品やアプリとも相互接続して新たな価値を創出する考えもある．当然のことながら，他社との相互接続戦略は短期間で多種多様なシステムを実現して，飛躍的に多様な価値が創出できる期待がある一方，以下に述べる四つの大きな課題もある．

まずは，IoTシステム相互の整合性の問題である．筆者の一人は，過去に建築分野に於いて異なるメーカー等のシステムの相互接続の経験があるが，そこでは個々のIoTシステムが既にサイロ化（後述）しており，これらを統合的に制御するシステム構築は，通信プロトコルなどに関する技術協議に加え利害調整も必要となるなど極めて煩雑な問題が横たわっていることを経験している．

この旧くて新しい問題に対する一般的な解決策は標準化である．標準化は異なるシステムの一部を関係者が統一するのであるから，本来は協業領域であるはずであるが，実際には自社が推す仕様がビジネス上優位になることを狙っ

て，主導権争いともいえる競争領域になってしまうことが多い．結果的に，標準化は多大な時間を要することが多く，その間に強い競争力を有する，例えばビッグテックと呼ばれる世界的巨大IT企業などは独自路線を進め，寡占状態が進んでしまう懸念も生ずる．

また，IoTは“あらゆるもの（以下，モノとも記す）がネットに繋がる”という概念であるから，2千円の扇風機や，100万円の玄関ドアなどモノの価額帯にも大きな幅がある．モノをConnectedにするには，当然何らかの増分コストが発生するが，本体価額に大きな開きがあることに起因してConnected化コストの負担能力にも自ずと開きが生ずる．すなわち，相互接続のための標準として単一の通信プロトコルを決めたとしても，このコスト負担能力に適合しないケースも発生することとなる．このような実情に鑑み，標準化という方法に依らず，多大な労力なしに異なるIoTシステムを相互接続する方法への関心が本研究の背景である．

次なる課題は，システム全体が上手く動作しない場合の対応についてである．これは，障害発生の際の初動を誰が行うのか，という“障害切り分け”問題とも言える．異なるメーカーやサービス提供事業者の機器やアプリを複合的に相互接続したシステムに於いて，全体として不具合が発生した場合，故障探索を関係事業者が一斉に行うことは当然効率的ではない．特にIoTの場合，モノがエンドユーザー宅などのいわば現場にあるため，障害対応にフィールドエンジニアの現場出向が必要になるなど，コスト増の要因を抱えている．まずは，どの事業者の責任範囲に不具合の原因がありそうか見当をつけ，当該責任範囲を受け持つ事業者が初期応動をすることが肝要である．具体的には，相互接続されているIoTシステム間に明確な責任分界点を設定できるようなアーキテクチャーを採用し，責任分界点を意識した障害切り分けをすることが大変重要である．

IoTシステムの相互接続には，さらに問題がある．データ利活用社会構築が提唱されるなか，「第三者に自分のシステムの稼働データを勝手に使われるのではないか」という不安問題が存在する．これには明示的，暗示的なケース両方があるが，この懸念は大変根強いものであり，IoTシステム相互接続の課題として，前述の「システム間の整合性」「責任分界点と障害切り分け機能」に加え，三点目としてこの「データ流通に関する不安」を挙げたい．

ビジネス上の問題はさらにある．第一の問題と逆説的になるが，相互接続がやりにくい（一般的にはこれをサイロ化という）ということは一種の差別化方策の結果であり，これが競争力の源泉にもなっているということである．他社の機器やアプリと自社のそれらを組み合わせて新しい価値創造ができることは既に述べたとおりであるが，他社と自由自在に相互接続できる環境は，競合する第三者も同様の環境を手にできることを意味し，競争力の点からはたして歓迎すべきなのか，という問題意識が存在するのも事実である．筆者らはこれを四番目の課題として捉え「協調領域に於ける公正競争環境の維持問題」と呼んでいる．以上の四大問題を表1に纏める．

表1　IoTシステムの相互接続に関する問題点

#	問題点	概要	解決策の方向性
1	通信プロトコルなどの整合性	・価額帯が広いIoT分野では接続に関わる増分コスト負担能力に大きな開きがある ・標準化は時間が掛かりすぎることが多い	標準化に依らない方策の考案が必要
2	障害切り分け機能	・コスト削減のためIoTデバイスを設置した現場出向は必要最小限にしたい ・複数事業者のアプリや機器からなるサービスの場合、初動をどの事業者が行うかをまず知りたい	責任分界点を活用した切り分け機能実現が必要
3	データ窃用に対する不安	・IoT-HUBに流れるデータを勝手に見られ貯められて勝手に使用されるのではないかという懸念	「行為」をしないことを明確化する方策が必要
4	公正競争環境の維持	対等かつ自由自在に繋がることは、個別事業者の競争力を削ぐことに繋がる	IoT-HUBという協業領域でも公正競争環境が維持できる仕組みが必要

3．個別課題に対する解決策

3.1　システム間の整合性に対する解決策

筆者らは標準化に依らない方法として，身近にあるパソコンとプリンターの関係に注目した．我々は，自宅や職場でいろいろなパソコンやプリンターを使っているが，A社のプリンターとB社のプリンターの通信プロトコルは統一されていない．しかし，ユーザーである我々は，なんの不自由もなく，実際にそれらを使いこなしている．筆者らはこのような例をヒントに，IoTシステム間の相互接続にも同じような構造をインターネット上に大規模に構築すれば，相互接続問題は大幅に軽減できるのではないかと考えた．

産学連携先と様々な検討と実証を進めた結果，筆者らはIoT-HUBと名付けたインフラを開発[1)2)3)]した．アプリやIoTデバイスなどどのようなIoTシステムであろうとも，その通信プロトコルに対応した“ドライバー”と呼ぶ小さなソフトウェアを用意し，原理的にはそれを背中合わせに接続すれば相互接続できることになる．背中合わせの接続を成り立たせる基盤がIoT-HUBである．

原理は簡単だが，ここに工夫を要する課題が存在する．Connected機能を備えた機器（以下，IoTデバイス）は通常二種類あり，当該機器のメーカーが運営するプライベートクラウドに収容されているか，IoTデバイスがWi-Fiなどの通信機能を有し，何らかの通信プロトコルに対応できる機能を有しているか，のどちらかである．筆者らは，前者をクラウド収容タイプ，後者をローカル接続タイプと通称している．使い易い相互接続基盤を構築するには，このどちらのスタイルにも“ドライバーの背中合わせ”原理が適用できるようにする必要がある．このため，ローカル接

続タイプのIoTデバイスには，エンドユーザー宅などの現場に設置でき，ドライバーを支えるIoT-HUBの張り出し装置的な機能を用意した．使用する具体的な機器としては，PCやタブレットPCなど汎用的な機器がコスト等の面から適切である．

IoT-HUB本体と張り出し装置の両方で“ドライバー”が同じように扱えるようにするため，R-Edgeと名付けた構造を開発した．インターネット上のIoT-HUB本体上であれ，IoTルーターと名付けた張り出し装置上であれ，このR-Edgeはドライバーのソケットのように機能する．こうすることで，クラウド収容タイプ，ローカル接続タイプ両方が同じようにドライバーによって接続されることを可能とした．なお，IoT-HUB本体は，Function as a Serviceと呼ばれるパブリッククラウドサービスによって構築したバーチャルインフラとして社会実装されている．これによりインフラ構築コストを変動費化することができる．

IoTルーターは，あくまでもIoT-HUBの出入り口機能を現場に登場させる張り出し装置であり，IoT-HUBの一部である．ホームオートメーションなどでは，ホームゲートウェイ（以下，HGW）などと呼ぶローカルコントローラー的な端末を設置するアーキテクチャーを見かけるが，IoTルーターの位置づけはこのHGWとは根本的に異なっている．

アプリケーションは，一般にWeb APIと呼ぶインターフェイスを相手にすることが多く，特別なドライバーが必要なケースは少ない．しかし，相互接続先が多岐にわたり，それぞれの相手先に届けるコマンド書式等が多数になってしまう場合等には，“アプリケーション・ドライバー”と名付けたドライバーでこれらの差異を吸収してしまう方法も実装可能[4]である．この考えは，アプリや機器本体からドライバーに至るまでの“自分の責任範囲は自分の自由にできる”という一種の理想状態を保証する．以上の説明を総合したインフラ概要を図2に示す．

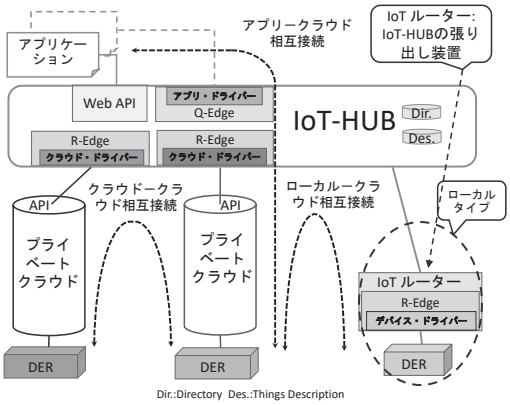

図2　IoT-HUBのインフラ概要

ドライバーは，IoTシステムの通信プロトコルに合わせたコマンドを送受信するように作る小さなソフトウェアであり，ソフトウェアエンジニア一人週程度の工数で製作可能である．IoTデバイスとのインターフェイス条件は，当該デバイスによって異なるが，① Webサイトなどで公開されている，② NDA締結を条件に提供されるよう準備されている，③個別協議を要する，であり，筆者らの実験経験ではConnectedデバイスは①, ②のタイプが多いようである．

3.2　障害切り分け機能の実装

ドライバーによる相互接続という概念を持ち込んだことにより，障害切り分け機能も比較的容易に構築できるようになった．生活に於けるPCユーザーの誰もが常識的なこととして，プリンターとプリンタードライバーは当該メーカーが一体として提供するものであり，プリンタードライバー以降プリンターまでは当該メーカーの責任範囲，と認識している．もちろんPCとプリンターを接続するUSBケーブルなどはその責任範囲外であることも共通認識となっている．

先のIoTデバイスとドライバーも同様でドライバー以降IoTデバイスまでがメーカーの責任範囲である，という責任分界点の在り方は上記の生活感的常識と整合性がよい．筆者らの実証実験では，ドライバーの背面（R-Edgeとの接合面）を責任分解点とすることは合理的である，と解してくれる関係者は多かった．このため，IoT-HUBではドライバーの背面を責任分界点と規定している．

IoTデバイスメーカーがドライバーを添付して製品を出荷するという機運に至るまではまだ時間を要するし，それまでドライバーはサードパーティー製のものとなることは必至である．しかし，前述の生活的なIT常識に立脚した関係者間の認識合わせにより，ドライバー背面を運用上の責任分界点とすることは可能である．

このようにドライバー背面を責任分界点とすることで，障害発生時の初動を誰が担うか，という問題はかなり判りや易くなった．さらに，これを可能とする機能もIoT-HUBには実装できることを確認している．図3にその原理を示す．情報伝達ルートを切り替えて試験することにより，障害が発生している区間の推定が可能になる．

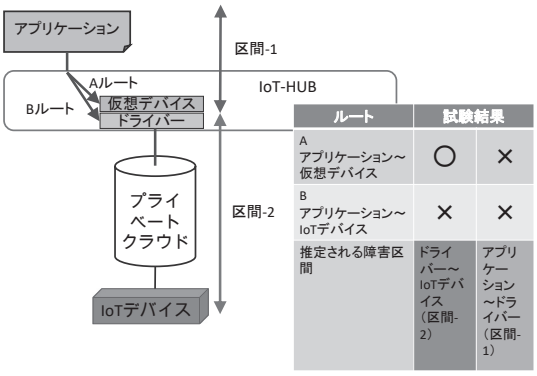

図3　障害切り分け機能の実装

具体的にはユーザーからの不具合申告を受けたサービス提供事業者は自身に許されたIoT-HUBの操作コマンドにより，障害発生の情報ルートを通常のBから，Aルートに切り替える．Aルートの先には，IoTデバイスからの応答をエミュレートする「仮想デバイス」が設置されている．「仮想デバイス」は応答をエミュレートするだけなので，実質的にはドライバーとさして変わらないソフトウェアである．このBルートとAルートの応答の違いから図3内の表のように障害区間が推定される．これをドライバー背面と規定した責任分界点と照らし合わせれば，初動すべき事業者が決まる．初動を担うのは，「サービス提供事業者」「IoT-HUB運営事業者」「IoTデバイスメーカー」の三者が候補である．実際には，前二者が一つのグループとして対応することとなろう．もし，障害がIoTデバイスメーカーの責任範囲であれば，当該メーカーはまず自身のトラブルシューティングツールを使って，自社の責任範囲内での故障探索をすると予想される．

なお，社会実装されたIoT-HUBではさらに先進的な機能を既に実装しており，提供するSDKによって製作したドライバーであれば，ドライバー等が命令に対して応答を返す機構を組み込まれるため，上記の原理的な切り替え方法に依らずとも，障害区間の推定が可能である．

3.3　データ流通に関する不安解消方策

IoTシステムの相互接続には，自身の機器等の稼働データがIoT-HUBの運営事業者によって覗き見られ貯められて，不当に利用されるのではないか，という拭いきれない不安がユーザー事業者側に存在する．この不安は，IoT-HUBのような結節点の機能的メリットを帳消しにするほど強いもので，納得感のある合理的な解決策が必要である．

そこで筆者らは，法規制を活用することを考案した．電気通信事業は，「他人の通信を媒介する」ものと規定[5]されIoT-HUBもその範疇に入る．電気通信事業法は，その第四条で（秘密の保護）電気通信事業者の取扱中に係る通信の秘密は，侵してはならない，と規定している．

IoT-HUBの運営者が電気通信事業者になれば，IoT-HUB利用者が抱えるデータ流通に関して不安視する行為自体が法令によって禁止されるため，この方策は明解な解決メッセージとなる．

3.4　協調領域に於ける公正競争環境の維持方策

IoT-HUBは，様々なIoTシステムの責任範囲を明確にした上で，相手と対等な立場で相互接続できる機能（以下，フラットな相互接続）と呼ぶことができる．この環境下では，競合他社も同様のメリットを得られるため，結局は自社の競争力を削がれることになるのではないか，という見方もある．この課題については，IoT-HUBの運営事業者が次のようなビジネススキームを採用することによって解決できる．

図4によって，クラウド収容スタイルを例に説明する．IoTデバイスの操作は，API（Application Program Interface）に信号を送ることによって行う．一般に一種類のIoTデバイスに対して複数のAPIが用意され，それぞれが機器の個別動作に対応したり，また，メーカーのトラブルシューティング専用などとなっている．

簡単のためZ社の同じモデルのIoTデバイスに対してA社，B社二社のサービス提供事業者が相互接続を希望しているものとする．Z社は，ビジネス上の損得勘定や相手の技術的レベルなどによって，A社，B社にアクセスを許すAPIの範囲を個別に決定すれば，フラットに繋がるIoT-HUB経由であっても，Z社-A社によるシステムと，Z社-B社によるシステムは差別化が可能となる．これは技術的マターではなくビジネススキームと呼ぶべき事柄であり，これを筆者らは協調領域に於ける公正競争環境の維持方策と呼んでいる．IoT-HUB運用者が，Webなどを活用してこれらの協議の仲立ちもすれば相互接続のワンストップサービスが実現する．この方策の社会実装は今後である．

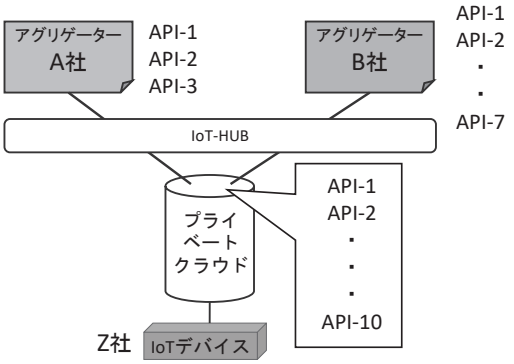

図4　協調領域に於ける公正競争環境の維持方策

4．活　用　事　例

4.1　基幹システムの柔軟性確保方策として

本インフラは，産学連携先によって2019年に社会実装され，現在実際の顧客によって活用されている．図5はいわゆるゼネコン企業による活用例である．この企業は，建設したビルのエネルギー管理や情報通信システムなど付帯設備の統合管理運用を建物OSと呼ぶ基幹システムによって積極的に進めている．付帯設備には，どのテナントも利用する基礎的なものに加え，テナントの好みによって選ばれる千差万別的なものもある．これらバラつきの多い案件に対応するために，基幹システムである建物OSを一々改修していたのでは，長い対応時間やコスト増を招くことは明白である．この応用事例では，このように柔軟に対応すべき付帯システム対応部分を一部IoT-HUB経由にすることによって，基幹システムの改修をせずに実現することを

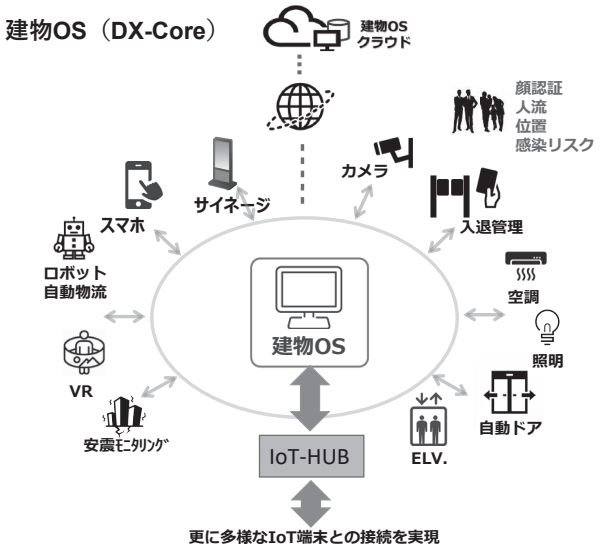

図5　ゼネコン企業による応用例[6)]

可能にしている．

4.2　既存経営リソースの活用ツールとして

図6は，リース会社での活用事例である．リース会社は顧客企業に於いて使用されているリース機材の把握のため移動体通信端末を多く利用している．LPWA（Low Power Wide Area network）など近年の技術進展による低廉な通信システムの登場によって，上記の通信コストを低減できる機会が訪れている．しかし，これを利用するためには，既存の管理システム全体を作り直す必要などをシステムベンダーから提案されることも多く，結果として却ってコスト高になってしまう悩みを抱えていた．

結果的にこの企業は，既存の管理システムはそのままにして，携帯電話システム（4G）からLPWAシステムの接続部分にIoT-HUBを介在させてプロトコルを変換し，システム改修コストを極小化しつつ，かつ，通信コストも低減することに成功した．いわばこれはBPR（Business Process Reengineering）の成功事例である．

5．お　わ　り　に

本インフラの相互接続対象には制限は特にない．カーボンニュートラルに寄与できる分散エネルギー資源なども対象とすべき重要なIoTシステムであろう．これには，ミクロなカーボンクレジット取引なども付随させるなどすれば[7)]，エネルギー領域に留まらない複合的なサービスの実現も可能となろう．

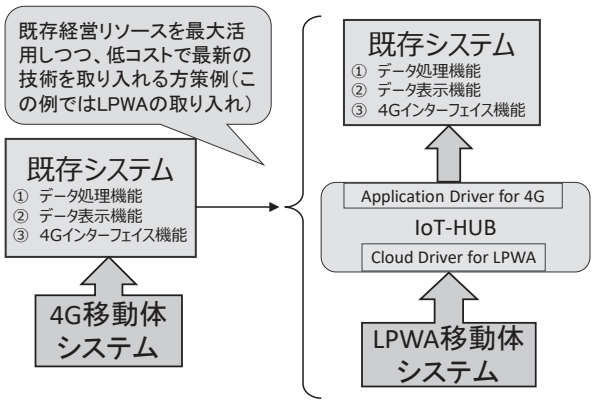

図6　リース企業による応用例[6)]

本研究は，2015年に設置したIoT特別研究会のメンバー企業のお力添え，また，同研究会と協業協定を締結し様々な実証試験を行って下さった団体さまのご助力によって実現できた．改めてここに謝意を表明する．さらに，研究成果を社会実装して下さったIoT-EX株式会社の小畑至弘，松村淳両代表取締役には格段のお力添えを頂いた．改めてお礼申し上げたい．

（2022年2月14日受理）

参　考　文　献

1）馬場博幸他，電力取引システム活用による離隔地点間における個人の余剰電力利用スキームの試験実装，電気学会論文誌C，Vol.141，No.3（2021），pp383-393
2）馬場博幸他，IoT向け多種システム相互接続インフラの開発，2021電子情報通信学会総合大会，D-23-11
3）馬場博幸他，IoT向け相互接続インフラの他網接続機能の追加，2022電子情報通信学会総合大会，D-23-3
4）馬場博幸他，DERの情報多様性要求への対応策検討，2022電気学会全国大会，4-164
5）電気通信事業法第二条
6）生産技術研究奨励会IoT特別研究会（RC-88）パンフレット（2021）
7）野城智也，建築分野におけるカーボン・トレーディング導入の道筋・意義，生産研究，73，4（2021），pp247-251