IoT 早期実現に関する業界内、及び、業界間の問題（参考日本語訳）

馬場博幸，東京大学
石田慶樹，日本インターネットエクスチェンジ㈱
天津孝之，東京電力㈱
國武功一，㈱ブロードバンドタワー
前田薫，㈱レピダム

要旨

本稿は、IoT を実現するにあたって、ICT 事業者のみならず、実際に工業製品を製造している事業者や社会基盤を構築・運用している事業者(以下「Things を扱う事業者」と呼ぶ)が、どんな問題を抱えているかをヒアリング調査し、まとめたものである。ヒアリングにより、Things を扱う事業者は、自社の製品寿命と ICT 技術の世代交代間隔の大きな開きや、電波伝播距離のカタログ値と実際の値との違い、さらには、あまりにも多くのセンサー類の設定などに戸惑っている姿が鮮明になった。IoT 実現のためには、その効能提唱によるサービスオリエンテッドなアプローチのみならず、このような地味な問題解決が同時並行的になされなければならないと考える。

１．　はじめに

IoT 実現に向けた規格の提唱など、多くの取り組みが多方面で推進されている。また、IoT がもたらす経済・社会へのメリットを分析・予想した報告なども多くあり、さながら、インターネットの効能が盛んに議論された 20 世紀末を髣髴とさせるようである。

筆者らは、IoT 早期実現のための課題を明確化することを目的に、以下のアプローチを試みた。まず、プレイヤーを、便宜的に IT 界のプレイヤーと、Things 界のプレイヤーに分けた。そして、IT 界、Things 界の主要なプレイヤーに会い、IoT を実現するにあたり、プレイヤー自身の内なる課題に加え、IT 界、Things 界それぞれが、他方に対しどんなことを課題として捉えているかをヒアリングした。

ここでいう IT 界のプレイヤーとは、通信キャリアや、IT 機器ベンダー、インターネットサービスプロバイダー、アプリベンダー、あるいはソフトウェアハウスなどを指す。また、Things 界のプレイヤーとは、住宅や住宅設備メーカー、鉄道や電力などのインフラ事業者、さらに、エアコンや冷蔵庫といった、俗に白物家電と言われる家電品のメーカーであって、これらは IT のユーザーという側面も有する。

本稿は、そのヒアリング結果を纏めたものである。したがって、IoT 世界を俯瞰し、そのメリットを説くようなマクロな提言ではなく、IoT におけるサービス実現のためには、どのような課題が存在しているか、というミクロなケーススタディの提示となっている。

２．　技術的問題

２．１．　セキュリティの確保とプライバシーへの配慮に関する問題

２．１．１．セキュリティの確保に関する問題

IoT 機器・デバイスを用いたサービスのセキュリティに関しては、次の二つの視点があることを確認した。一つは、IoT が重要インフラに関わることで顕

在化するセキュリティである。二つ目は、個人や家庭のセキュリティである。

一つ目の重要インフラに関わるセキュリティにおいては、これまではセキュリティを確実なものとするために、インターネットなど外部のネットワークには物理的に接続せずに隔離するというポリシーが貫かれてきた。しかし、面的に広がる膨大な設備のリモートメンテナンスや、故障予兆の把握のために、独自仕様からオープンな IP プロトコルを用いた仕組みの整備が進んだことに加え、様々な目的達成のために外部ネットワークとの接続もやむえない時代が来ている。また、直接的な接続がない場合でも、すでに国際的なサイバーテロの標的とされていたり、内部犯行や標的型攻撃などの流行を考慮すると、セキュリティ上のリスクに大きな変わりはなく、隔離ネットワークにおいても同様の考慮が必要なことは明白である。社会インフラにおける IT セキュリティは、その影響度から、極めて高いレベルのセキュリティ確保が必要となる。

二つ目は、個人や家庭などのミクロな単位のセキュリティである。IoT の導入によって利便性が高まるとともにリスクも高まる。
例えば、玄関ドアがネットワークに繋がっている、という製品がすでに存在している。IT のセキュリティ技術においては、暗号鍵の桁数を増やして実質的に破られないようにしてあるものがある。しかし、設置時にどんなに最新のセキュリティ技術を導入しても、玄関ドアの耐用年数が 20 年～30 年ということを考えると、途中で陳腐化さらには危殆化してしまう。他の項目でも出てくるが、IT 的な時間感覚と、Things 的な時間感覚は、完全に異なる場合がある。

２．１．２．取得したデータに関してプライバシーの問題

取得したデータの取り扱いに関するプライバシーの問題は、IoT を推進している企業にとっては非常に大きな問題となっている。また、データは誰のものなのかも、もう一つの問題である。

例えば、鉄道事業会社においては、駅の安全のためであったり、飲料の自販機のマーケティングのためであったりと様々な形でカメラを設置しているが、かならず個人の識別とプライバシーの問題が出てくる。現時点では、事業者はリアルタイムで画像を処理し、ストレージしないことでこの問題を回避しているようである。

もう一つは、データは誰に帰属するのかである。これまでは、事業者のものか、ユーザーのものか、という二分法的議論がなされてきたが、さらにユーザーという小さい集団の中にも、多種多様な関係があり、ことはそう簡単ではない。例えば具体的な事例としては、HEMS の実験を行った事業者が、そのデータの扱いについて、設置した家の世帯主にそのデータの利用許諾を

得たケースがある。このケースでは、後日、その配偶者から許諾について異議が挙げられ、その家に対する許諾そのものが結果的に得られなくなってしまった。

２．２．　データの取得、配信とデータの管理とデータ量の問題

２．２．１．トラフィック・パターンの問題

IoT 機器・デバイスからのデータの取得、それらへのデータの配信はこれまでのインターネットの利用のトラフィック・パターンと大きく異なってくる。これまでのインターネットでは、情報配信に特化しており、コンテンツを人間に効率よく配信するような構造になっていた。それに対して、これまでの比ではない多種・多様なセンサーやデバイスへの定常的あるいは非定常的なデータの送受信は、これまでのインターネットトラフィックと大きく異なることが予想できる。しかしながら、どんな Things がどのくらいのトラフィックを送出し、それがどのように重畳されるのかという予測は十分に行われていない。また、具体的にこのトラフィックを運ぶ、バックボーンの設計や運用について具体論の説明はなく、また逆に通信事業者側では IoT のトラフィックのための必要な諸元が明確ではないケースも多いため、具体的な設計を行うことが難しい状況にある。

さらには、IoT 機器の設定、管理においても課題があり、建設関係の事業者からは、多数設置するセンサーなどの IoT 機器に対する設定作業だけでも大変な労力を要する、ということを聞くことができた。

２．２．２．取得した大量のデータの問題

取得したデータを安全で効率よく再利用可能に管理する手法の開発が必要である。現在でも、人間に紐づいた社会的データ（ID など）がハッキングされ漏洩するという事件が時折発生している。IoT 時代は、それに加えて Things に紐づいたデータが大量に発生し、さらにそれらが個々の人間と紐づいていくことも多くなる。政府機関や大企業ほどは IT システムに多くの投資が行えない者も、IoT 界のプレイヤーである。このようなプレイヤーでも、取得したデータを安全で効率よく再利用可能に管理する手法の開発が必要である。ID の管理スタイルや関連する法規制は国や地域によって全く異なっており、この問題も、社会と個人の関りに関する常識の違いに大きく左右されるため、ローカライズが必要になる。

２．２．３．データの爆発的増加と多様性の問題

今後の IoT 時代には、センサーや IoT 機器から多種多様なデータが送出されることとなり、データ量の爆発的増加に対する懸念がある。一方で、所謂 M2M 通信は、映像のような大容量のデータが必須ではないので、センサー数の増分と比してもトラフィック増加度合いはさほど驚くようなものではないとの見方もある。

ありとあらゆる Things からデータが送出されることとなると、その種類は

数えられるというより、数えられないと表現する方がいいだろう。さらに、現在のインターネットトラフィックは、人間を受け手と想定しており、また動画や画像などのダウンロードが多いことから、アップロードのトラフィックとの間には数倍の開きがある。IoT の中でも M2M 通信と言われるタイプが大幅に増えた場合、この上り下りの開きはいまほどではなくなる可能性があり、ネットワーク、特にラストワンマイルの特性には根本的見直しが要求される可能性がある。この点についての問題意識はまだまだ低い状況にある。

２．３．　物理世界と仮想世界のマッピング

２．３．１．取得したデータの物理的な対応の問題

取得したデータは単なるデジタル値であって、それが具体的に何を意味するか対応付けが必要である。多数設置されるセンサーなどの IoT 機器に対する設定だけでも大変な労力を要することは先に述べた。さらには、そのデータが何を意味するのかという現実世界との紐付けも膨大な作業量となってしまうのが実情である。

エネルギーマネジメントの実験の現場においては、その対応付けを人が行っているために手間もかかりまたミスが入り込む可能性がある。現段階ではこのように人間の手作業に頼っているような事柄も、いわゆる自動設定的な仕組みを構築して、IoT 導入の手間やコストの削減や人を原因としたミスの排除ができるようにする必要があろう。

２．３．２．データのキャリブレーションの問題

さらに、Things から出てきたデータが、当該 Things そのものときちんと紐づいており、その動作状況を正しく表現しているかのキャリブレーションも重要である。

前項は、IoT 機器の導入、本項は運用継続のためのものであるが、これらをパッケージとして可能とするツールが必要となるのではないだろうか。

２．４．　製品の寿命と世代管理、機器更新のためのコスト

２．４．１．製品寿命の問題

IoT 機器・デバイスの製品寿命は 10 年以上となっているのに対して ICT 機器のそれは 5 年以内程度が多く、ミスマッチがある。

ネットワークに繋がった玄関ドアの例をすでに挙げたが、玄関ドアは、一度設置すれば、20 年～30 年と使用することはごく普通のことである。一方で、このドアや、ドアについている鍵をネットワークに繋ぐ場合を例に考えてみよう。そのネットワークに接続する通信技術や通信サービスは、ドアを使用している 20 年～30 年の間に、何度も世代交代してしまうのが常態化しており、ここに IT 界と Things 界の大きなギャップが存在する。

この問題に関して、住宅設備メーカーからヒアリングによって得られた解決策の一例を以下に示す。例えば、建物にある複数のシャッターを自動制御するような場合、コントローラーから複数のシャッターに至る部分は、いわ

ゆる枯れた技術でシャッターメーカーが担い、コントローラーがネットワークに繋がって通信サービスの世代交代に対応するという形態を取ることである。

２．４．２．コモディティ機器への IoT の導入の問題

世間に普及している様々なコモディティ機器を IoT 機器・デバイスとして利用可能とするためには多大なコストを要する。コモディティ機器を IoT 化するためには、二つの方法をとり得る。一つは IoT に対応した機器に更新することでる。二つ目は、コモディティ機器に付加する何らかの装置を用意するかのいずれかの方法となるが、いずれも費用が発生する。いずれの手法をとるにしても、費用の負担を乗り越えるための何らかのインセンティブが働かない限り、IoT の導入には長期間の時間を要することとなる。

２．５．　関連規格の標準化のスピードと多さの問題

２．５．１．関連規格が多い問題

IoT 機器・デバイスに組み込むに適した規格が多数存在する。例えば、通信技術をとっても、Bluetooth、WiFi、NFC、LTE など多くの規格、技術、サービスが存在する。このうちの何を選択するかを決めることは困難が伴う。

IoT、特に Things 界のプレイヤーは、必ずしも通信技術のプロを擁しているわけではない。ヒアリングでは、こういった自身の専門領域とは異なる分野に関して、戸惑う声が複数聞かれた。もちろん、いろいろな技術が競争して、その品質や完成度を高めていくことはユーザーにもメリットをもたらすことであり、それを否定するものではない。

Things 界事業者に対し、ICT 技術を判りやすくコンサルテーションするような仕事が今後出現するかもしれない。また、複数の規格を相互に接続するための仕掛けのようなものがあれば、Things 界からの IoT へのアプローチも加速するだろう。

２．５．２．標準化のスピードの問題

IT 界と Things 界では製品の寿命に関する考え方が根本的に異なる。このため、標準化についての考え方も大きく異なっている。IT 界においては様々な提案の中から適当と考えられる標準化を進め、また一度決定したものを更新する場合も多い。そのような標準に追従するために製品を更新することを厭わない。一方の Things 界において、製品は長寿命を持つためにできる限り安定的な標準を組み入れることを希望するが、枯れた標準化を決定するには大変な時間を要する。Things 界の製品に IT 界の標準を組み込もうとする場合に、標準が流動的でなかなか決まっていないように見えることになる。また標準化に関しての働きかけを行おうとしても、標準化のプロセスが異なっているためになかなか対応できないというのが現実である。

２．６．　相互接続性と責任分界点と全体としての品質保証の問題

２．６．１．相互接続性の問題

マルチベンダーで構成されることによりインターオペラビリティの検証をどうするかは大きな問題となる。インターオペラビリティは、大変重要な課題である。機器同士のインターオペラビリティに加え、バックワード・コンパチビリティの確保も IoT 実現のためには重要である。

これらが担保されないと、過去の製品も含む IoT 世界は実現し得ないだろう。

２．６．２．障害切り分けの問題

何らかの問題が起こった時の障害切り分けをどのように行うかも問題である。個人の PC の利用において、多くの人が障害を経験しているが、その障害の切り分けは個人が行う必要があり、誰も面倒は見てくれない。

IoT 世界では、ことはより一層深刻度を増す。スマートハウスという IoT のユースケースの一つを捉えても、エアコンや風呂、ドアなどがネットワークで繋がり、何らかの障害でそれらが機能できなかったとすると、エンドユーザーに強いられる不便は、PC の障害において電子メールが送れないという障害レベルよりはるかに大きいものとなる。

障害切り分けをユーザーの責任で行う必要があるとすると、うまく切り分けることができず、どのメーカーに修理を頼めばよいのか分からない、あるいはメーカーに修理を頼んでも自社の責任ではないと修理を断られてしまう、といった事態が想定される。この例からも判るように、この問題の解決は、B2C 的な IoT が実現できるかどうかを決定づけるほど重要な課題である。

２．６．３．品質保証の問題

個々の IoT 機器・デバイスの品質保証が、全体の品質を保証することにはならない。いくつもの Things や通信が繋がるのだから、全体のサービス品質は、容易にボトルネックとなる IoT 機器・デバイスの品質レベルにまで下がってしまうと考えるのが自然であるが、利用者にはそのことは意識されない。また、２．６．２に記したような一つ一つの構成要素の品質とは直接関係無い問題が、サービスとしての品質を決める重要なファクターになってしまう問題もある。このように、IoT の品質問題は、個々の Things という点で決まるのではなく、それらがネットワークされた面的広がりを持ったサービスとしての品質問題であると捉えられる。

２．７．　製品の設計ポリシーの問題

２．７．１．設計ポリシーの変更の問題

これまでの単体製品の高機能化から、個々の製品を単機能化し、他製品などとの協調性を持たせる設計ポリシーへの転換が必要である。

これまでの Things 界は、機器の品質向上とともに、如何に製造物を高機能化し、付加価値を付けるか、ということをテーマに長年注力してきた。これに対して IoT 時代は、Things は極力基本機能に絞り、Things 間で協調を図る

ことにより今までにない付加価値をアプリケーションという形で外出しにすることを暗黙の前提としている。そして、その単純化された Things は、同じアプリケーションで他の事業者の Things も動作できるよう求められる。

このように IoT 時代は、今までとは全く逆のポリシーをとることを Things 界に迫ることになる。製造業者からのヒアリング結果からは、その理解、転換の難しさがうかがえた。

２．８．　実際の利用面における様々な技術的制約の問題

２．８．１．電波を利用する際の問題

IoT において電波を利用する際の課題(到達範囲、利用可能な想定範囲よりも飛ぶ／飛ばない)があるという意見を、様々な局面で耳にした。IoT を構築するサプライヤやプロバイダは、必ずしも通信技術に長けているわけではない。電波の専門家以外は、電波は送信アンテナから、受信アンテナに一直線に飛んでいく、障害物があれば、それで遮られる、という絵のようなイメージで考えているようだ。だから、何メートル飛ぶ、とか、飛ばないか、という質問が繰り返されることになる。発射された電波は様々な場所で反射し、これが受信点で重畳されて受信される、反射の状態変化によって、フェージングと呼ばれる受信強度の変動が起こる、などを理解している人は少ない。このような専門的問題に対する、アドバイスする適切なポジションの技術者の欠如が問題となっている。

２．８．２．バッテリーの問題

バッテリーの利用可能時間と寿命も問題となっている。これも、本質的には電波到達距離問題と同じである。カタログスペックと実際の差異がどの程度であるか、使用環境など多くのファクターによって、バッテリーの持続時間は変わるだろう。要するに専門家でも難しい問題を、IoT 事業者という、いわばユーザーが解く必要があるのかも知れない。

２．８．３．配線の問題

配線の多さ・複雑さ(電力線と通信線)が問題となる。大量のセンサー、機器、そして、それらを駆動するための電源線、情報を取り出しネットワークに繋げるための通信線など、IoT 実装に際しては、ワイヤーハーネスが欲しくなるくらいの煩雑さがある。さらに、通信線を工事する技術者と、電力工事する技術者は別々であるケースが多く、問題を煩雑にしている。

２．８．４．オープン化の問題

IoT 商材は一社による実現は不可能であり、オープン化して、様々な業種が協業しないと実現できない、と言うのが現実である。これまで、Things 界においては、製品はクローズドで開発して、自社製品によるユーザーの囲い込みを行ってきたために、製品をオープン化して相互接続性を持たせるという設計思想はなかった。このため、これまでの設計思想を 180 度転換して、競

合他社の製品とも相互接続性を有する設計に変更しなければならない。

３．　非技術的問題

３．１．　製品パラダイムの変更の問題

３．１．１．エコシステムの破壊の問題

IoT の導入によって、企業や業界のエコシステムを、場合によってはいったん破壊する可能性がある。もちろん、破壊が主目的ではないが、新たな価値の創造に関して、今までの製造業のような垂直統合型の Things 作りでは、時間やコストがかかりすぎる時代になりつつある。また、他のカルチャーを有する者のアイデアの取り込みも難しい。このパラダイムシフトの必要性は、容易に理解できることではあるが、難しい経営問題でもあるだろう。

３．１．２．協調、そして、戦略の大幅な変更の問題

競合者や他業種との協調、協力、新たなパートナーシップの提携が必要になる。これも、これについてはみな充分な認識はあるものの、具体的な実現へのハードルは非常に高い。

例えば、ちょっとした意見交換時に必要以上に情報を制限したり、用語や文化の違いによりコミュニケーションがうまくいかないという事例があるようだ。

３．１．３．既存産業との競合の問題

ビジネスモデル変更・改革を進めた場合によく出てくるのが、この既存産業との競合問題である。この問題は既存産業との競合というよりも産業の再編とみることができるが、スーパーバイザがいない環境下で産業の再編を進めることは難しい。

３．２．　メリットの問題

３．２．１．コスト上昇の問題とマネタイズ

IoT 化により製品そのもののコストが上がるのに対して効果が見えない、具体的なキラーアプリが不在で直ちに利用が増えるように思えない。利用が増えないなために、提供者側の負担を賄うためのマネタイズの手法も見えない。特に、コストダウンによる低価格化が主な競争要因となっている業種・製品ほどこの問題の影響が大きいようである。

３．３．　社会制度的な面でのセキュリティとプライバシーの問題

３．３．１．データの所有と所在と利用の区分の問題

IoT 機器から集まる多種多様なデータは、誰に帰属し、どこに保存し、誰に利用許諾を与えるのか、社会に受け入れられる仕組みが必要とされる。

例えば、開閉データが取得できるドアを事業者が家に設置した場合、その

開閉データはユーザーのものなのか、事業者のものなのか、あるいはこのデータを別の事業者も利用してよいのか、といった問題がある。

３．４．　データの開示の問題

３．４．１．データ開示への副作用や悪意への問題

データ開示そのものが個人や社会に対する安全・安心への脅威となる可能性がある。

例えば、電力のスマートメーターでは電力がいつ使用されているか、逆に言えば、いつ使用されていないかで留守がわかってしまい、空き巣に狙われるという副作用が以前から指摘されている。やはり、セキュリティとプライバシーの確保については、充分な手を施す必要があるという判りやすい事例である。

３．５．　社会的需要対応への準備の問題

３．５．１．法規制

法令による規制や規律は、従来の製品による生活の安全性を維持している重要な枠組みではあり、これを否定するものではない。しかしながら、イノベーションにとっては、障壁となることはよくあることである。

IoT では、国内法だけでなく、海外の法律など、さらには国をまたがった規制など、様々な法や規制が関係する可能性がある。規制当局も、IoT をよくウォッチして、グローバルな競争環境の中でネガティブな影響を与えないように自らが所掌する規制や規律を適宜ファインチューニングするなどの行動が求められる。

３．５．２．企業のコンプライアンスへの対応の問題

企業の IoT 推進に当たっては、自らの利益を追求するだけではなく、社会的要請への対応やユーザーの利益を同時に高めるものでなくてはならない。

３．５．３．個々のユーザーにあわせたカスタマイズの問題

万人向けの製造物から、個体向けにカスタマイズされた製造物への変化が求められている。

製造業のサービス業への転換とも言えるかもしれない。これには、IoT はかなりの役割を果たせるであろう。マスプロ的に Things をつくるより、機能の一部をアプリケーションとして外出しすれば、カスタマイズがとても容易になるだろう。これを実現するには、同時に、製造業側のパラダイムシフトが必要なのは前述のとおりである。

３．５．４．ユーザーのリテラシーの問題

Things が、ネットに繋がる以上、アプリケーションが存在し、一部はヒューマン・インターフェイスとなる。これからの IoT 時代では、ユーザーも IoT アプリケーションに対するリテラシーが必要となろう。

３．５．５．個人と家庭の分別の問題

家庭にあるThingsのデータが個人に帰属するのか家庭に帰属するのかにより、データの解釈やプライバシーの問題が大きく異なる。

２．１．２．でも述べたとおり、世帯主がデータの利用許諾をしても、その配偶者が異議を唱えるケースもある。

４．　セキュリティについての考慮事項

IoT に関わる様々な分野のプレイヤーにヒアリングした結果から、セキュリティ上の課題として明らかになったものを、以下のセクションで述べている:

* ２．１．１．　デバイスへの物理的タンパ
* ２．１．１．　製品寿命と暗号強度

各問題の詳細については対応する本文を参照。

５．プライバシーについての考慮事項

同様に、プライバシー上の課題として明らかになったものを、以下のセクションで述べている:

* ２．１．２.、　３．３．１．　データは誰に帰属するのかの問題
* ３．４．１．　データ開示と悪用の問題
* ３．５．５．　個人と家庭の分別の問題

各問題の詳細については対応する本文を参照。

以上