6. IoT をめぐる現在の法的環境について

弁護士法人　ALAW＆GOODLOOP
弁護士　吉井 和明 様

1）はじめに

IoT（Internet of Things）は、1999 年当時、Procter & Gamble（P&G）にいた Kevin Ashton が P&G のサプライチェーン管理へ RFID を活用することに関して使った言葉と言われている[1]。

しかし、その後、この言葉は、「あらゆる物がインターネットを通じてつながることによって実現する新たなサービス、ビジネスモデル、またはそれを可能とする要素技術の総称[2]」などと相当広い意味に用いられるようになっている[3]。

このような状況は、当初バズワードと言われながら、今では用語として定着したクラウド・コンピューティングにも似たようなところがある。もっとも、およそ物とインターネットがつながるものをすべて含むということであれば、その意味は限りなく広がり、その範囲はクラウド・コンピューティングの比ではないかもしれない。そこで、IoT そのものについての法的環境整備や法的解釈はあまり意味を持たず、結局のところ、IoT の用途ごと、ケースごとに応じて、法的問題点を分析したうえで、それぞれ解決するしかないということになる。

もっとも、IoT 全体について、共通の要素は存在し、また、その用途をある程度のグループに分けた場合にも、グループごとに共通の要素を抽出し得るとも考えられる。

それらの要素の抽出、及び個別の要素に関して、既存の法律で対応できるのか、できるとすれば、どのように解釈していくのか、できないとすれば、どのような法的環境を整えていくべきなのかが盛んに議論されているのが現状であり、未だ流動的である。

これらに関しては、各省庁での検討も数多く行われおり、本稿では、これらの検討を横断的に分析し、IoT をめぐる現在の法的環境を浮き彫りにすることを目標としたい。

2）IoT の法的環境を考える上で考慮すべき事象について

IoT をめぐる法的環境を考える上で、そもそも、IoT における、どのような事象が問題となるかを検討する必要がある。

1　RFIDJOURNAL 2009.6.22 記事 <http://www.rfidjournal.com/articles/view?4986>
2　デジタル大辞泉「IoT」
<https://kotobank.jp/word/IoT-676428#E3.83.87.E3.82.B8.E3.82.BF.E3.83.AB.E5.A4.A7.E8.BE.9E.E6.B3.89>
3　特定通信・放送開発事業実施円滑化法附則 5 条 2 項 1 号では、「インターネット・オブ・シングスの実現（インターネットに多様かつ多数の物が接続され、及びそれらの物から送信され、又はそれらの物に送信される大量の情報の円滑な流通が国民生活及び経済活動の基盤となる社会の実現をいう。）」と定義されている。また、平成 28 年 12 月成立した「官民データ活用推進法では、同法における「インターネット・オブ・シングス活用関連技術」について、「インターネットに多様かつ多数の物が接続されて、それらの物から送信され、又はそれらの物に送信される大量の情報の活用に関する技術であって、当該情報の活用による付加価値の創出によって、事業者の経営の能率及び生産性の向上、新たな事業の創出並びに就業の機会の増大をもたらし、もって国民生活の向上及び国民経済の健全な発展に寄与するもの」と定義する (下線部は共通部分)。間接的な定義であるが、参考となる。

これに関しては、IoT の仕組みに関して分解して考えると、大まかには、①IoT 端末に関して生ずるもの、②IoT 端末から処理を行うサーバー等への通信に関して生ずるもの、③処理を行うサーバー等処理装置やサービスに関して生ずるものの３つに分けられるように思われる。

このうち、①IoT 端末に関して生ずる問題としては、データのやり取りによる誤作動を含む、当該端末の物理的安全性の問題、挙動などの悪用の問題、電波政策の問題、知的財産権の問題が挙げられる。なお、ここでの物理的安全性に関しては、情報分野におけるセキュリティの思想だけでは通用せず、セーフティの考え方が必要であるとされる[4]。

②通信に関して生ずる問題としては、情報セキュリティ（完全性、可用性、機密性）、通信の秘密、プライバシーの問題が考えられる。

③処理装置やサービスに関して生ずる問題としては、ビッグデータの問題としての情報処理や情報流通の問題、さらに AI にまつわる問題も含まれ得る。

なお、これ以外にも、利用の用途に応じて、各種業法などの取り締まり法規との抵触に関する問題が生じ得るし、システムの構築全体の問題として、システム開発における諸問題が生じ得る。

3）IoT 端末（Things）に関する法的環境について

① 端末自体の安全性

IoT 端末の物理的安全性としては、IoT 端末自体の不具合によるもののほか、サービス側からのデータにおける不具合により生じた誤作動も考えられる[5]。

また、長期間使用されている IoT 端末に対して、何らかの外部からの攻撃が加えられ、これにより乗っ取られて踏み台と化し、これにより、他の端末に攻撃が加えられ、あるいはデータを漏えいするなどと言ったことが考えられる[6]。

加えて、データの残された端末や、データ通信可能な端末が安易に廃棄されたことにより、端末内の情報が漏えいするといったこともあり得るだろう[7]。

このように、機器自体の安全性が問題となったことにより、IoT 端末メーカーや、システム・サービス事業者がユーザーに対して責任を負うことが想定されるほか、これらにより第三者に損害が生じた場合には、端末利用者自体が、その管理者として、第三者に対して責任を取られる可能性もある。

ここでの重要な点として、IoT において、Things の安全性は、Internet 側におけるセキュリティの考え方とは根本的に異なっているということである。

すなわち、Things の物理的な安全性においては、情報セキュリティにおけるベストエフォート、あるいはリスクマネージメントのような考え方とは異なり、基本的にリスクを織り込んだ設計を行うようなことはできない。

この点は、情報セキュリティの思考になれた Internet 側としては意識を転換し、Safety by Design の思想を取り入れていく必要があるといえる。

4　内閣サイバーセキュリティーセンター「安全な IoT システムのためのセキュリティに関する一般的枠組」＜http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf＞では、「モノが接続されることから、IT と物理的システムが融合したシステムとして捉える必要があり、同システムが提供するサービスには、従来の情報セキュリティの確保に加え、新たに安全確保が重要となる。」としているが、同趣旨と捉えられる。

5　2012 年には、US のセキュリティ研究者である Barbaby Jack により、ペースメーカーをハックし、830V の電流を送ることが出来るといった報告もなされている
＜http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html＞

6　総務省・経産省・IoT 推進コンソーシアム「IoT セキュリティガイドライン Ver1.0（案）」＜http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/dai2/siryou2.pdf＞（以下、「IoT セキュリティガイドライン案」という。）P.54 参照

7　端末の廃棄による漏えいは、これ自体は、IoT の問題といえるかは微妙であるが、電子機器の廃棄において、このような事件は現に発生しており、多数のユーザーの利用により、発生し得るリスクとしては、検討すべき内容といえる。

② 挙動などの悪用[8]

IoT 端末の挙動などを悪用される可能性がある。

例えば、総務省・AI ネットワーク化検討会議「ＡＩネットワーク化の影響とリスク ― 智連社会（WINS ウインズ）の実現に向けた課題 ―（報告書 2016）」（以下、「AI ネットワーク化検討会議報告書 2016」という。）の P37 では、親しみのある見た目の人型ロボットが、オレオレ詐欺の「受け子」や「出し子」など人間の代替物として犯罪に悪用されるリスクが挙げられているが、ロボットに限らず、IoT 端末を違法行為に役立てるために利用されるケースは考えられる。

③ 責任の所在

IoT においては、IoT 端末の所有者・管理者、IoT 端末の製造者、サービスの提供者など、多数の当事者が様々な役割を果たしている。

このように多数の当事者が関わる法律関係では、各当事者の責任の考え方も複雑になる。

例えば、IoT 端末の誤作動により、第三者に損害が及んだ場合、その損害について責任を負うのは、どの範囲の当事者なのか、どこまで責任を求償することができるのか、損害を被った第三者は、誰に責任を問うことが出来るのかということを考えた場合に[9]、簡単に答えが出るものではないことは容易に想像がつく。

④ 電波政策

IoT システムにおける大容量、低遅延、多数同時接続を実現する 5G 商用サービスを 2020 年に提供できるよう、標準化や 2017 年からは、総合的な実証実験を実施するとされている[10]。

今後、IoT に適した電波政策がとられるに従い、それに見合った環境も整備されていくことが予想される。

⑤ 知的財産権・データの帰属

知的財産権・データの帰属については、いくつかの課題がある。

IoT におけるデータの流通と当該データやライセンスの帰属の問題、及び、AI と結びついた場合に、これにより生成されたデータの利用等に関する権利の制度的整備である。

8　IoT セキュリティガイドライン案 P.16 では、海外では、不満を持った退職者が遠隔から自動車の管理サービスを不正操作し、自動車を発進できなくしたり、ホーンを鳴らしたりする事件や、銀行が管理する ATM の物理鍵を複製し、その鍵を用いて ATM の保守扉を開けてウイルスを感染させた上で、ATM の USB 端子にモバイルデバイスをつなげて現金を払い出させる事件などの海外での事案を紹介し、内部不正への対策が必要とする。

9　当該第三者が損害の賠償を求める場合、当該第三者は、自身の損害を回復できる可能性の高い方法を採るであろうから、実際には、回収可能性の高い当事者に対し請求を行う、あるいは当事者全員に対して、損害を求めるなどするであろうから、第三者にとって当事者選択の困難は存在しない。ここでの問題は、専ら、IoT を利用する側、提供する側において、どの程度のリスクを負うことを予測すればよいかということである。

10　総務省「IoT・ビッグデータ時代に向けた 新たな情報通信政策の在り方について 第三次中間答申」
＜http://www.soumu.go.jp/main_content/000461289.pdf＞P.5

前者に関しては、専ら、データの使用に関するライセンスの定め方や、利用条件、NDA（秘密保持条項）の定め方など、契約により解決するべきものと考えられるが[11]、データの内容により保護が難しい場合もあり、また、それが保護されるかどうかは、データの価値評価を必要とするため、一義的に判断することが困難な面がある。将来的に何らかの法的手当てを行うことで、取扱い方を明確化することもあり得るかもしれない。

後者に関しては、知的財産としての新たな権利の創設、不正競争防止法の営業秘密としての保護、モデル契約条項による整理等が検討されている、とされている[12]。また、一般財団法人知的財産研究教育財団知的財産研究所による平成28年度特許庁産業財産権制度問題調査研究書「AIを活用した創作や3Dプリンティング用データの産業財産権法上の保護の在り方に関する調査研究報告書vii以下では[13]、「(ⅱ)AIを活用した創作に関する法的論点」において、「自然人の発明であると認定する材料として、課題設定、解決手段候補選択、実効性評価のいずれかを人が行っていることが挙げられ、発明の着想・具体化を人が行っていることも、判断材料となり得る」としたうえで、これらの判断材料をどのように評価すべきかは、検討が必要であるとし、AIを活用した場合であっても、発明に関与した人の寄与度を個別に判断し、その発明に係る権利の帰属を決定していくことになると考えられる」とする。

当然ながら、これらの知的財産の帰属は、法的解釈を必要とするものであり、しかも、まだ定見をみないものであるから、上記報告書記載の材料が判断のために用いることのできる唯一の事実ではなく、また、権利の帰属の考え方も種々あろうが、一つの考え方として参考になると思われる。

4）通信に関する法的環境について

① 情報セキュリティ

電気通信であるため、この場面では、従来の情報セキュリティ（気密性、完全性、可用性）の確保が問題となる。

とられるべき施策がとられていなかった場合には、法的責任が生じ得る点でも、一般的な通信と同じである。

もっとも、通信の誤りや遅延等がIoT端末の誤作動につながり、物理的な危険を生じさせる可能性があることは上述のとおりであり、その面では通信といっても、IoT端末と一体となり、その安全性を確保する必要があるといえる。

② 通信の秘密

同じく、ここでは、一般的な電気通信と同じく、通信の秘密の確保が必要となる。

11　総務省・経済産業省・IoT推進コンソーシアム「新たなデータ流通取引に関する検討事例集 Ver1.0」（2017.3）＜http://www.meti.go.jp/press/2016/03/20170310002/20170310002-1.pdf＞では、「機器製造事業者が工場に設置したセンサーから取得した機器の稼働データを分析し、自社サービス（効率的な運転のアドバイスや予防保全等）で利用するとともに、第三者へ販売するモデル」における「センサーから取得した機器の稼働データの利用権」について、センサーにより取得したデータ自体がプライバシー侵害などにつながらない単なるデータである場合で、「工場から委託を受けて、センサーを設置し、事業を実施するのであれば、委託契約を結ぶ際、データの利用条件についても改めて契約を結びなお」し、「秘密保持契約ではなくノウハウのライセンス契約 や著作者人格権の不行使特約の規定を参考にするとよい。」としている。

12　「データ流通環境整備検討会　AI、IoT時代におけるデータ活用ワーキンググループ中間とりまとめ」P21。

13　http://www.jpo.go.jp/shiryou/toushin/chousa/pdf/zaisanken/2016_05.pdf

5）処理装置・サービスに関する法的環境について

① 個人情報

個人情報保護法制に関しては事業者の設置主体により適用法が異なるという問題がある[14]。

また、センサーなどで取得した情報が個人情報に当たる場合、それを第三者に提供するには、原則として本人の同意が必要となる（個人情報保護法２３条１項）。

この本人の同意を不要とするためには、統計情報として（提供者側でも復元できないようにする程度に）個人情報該当性を全く失わせてしまうか、改正後の個人情報保護法（本執筆時点では未施行）において、導入された匿名加工情報（個人情報保護法９条２項、各運用について同法３６条から３９条）とするなどの方法がある[15]。

個人情報該当性に関しては、例えば、カメラなどで取得した顔画像を認識し、これを数値化したものなどについては、個人情報の一内容である個人識別符号として取り扱われることとなる点に注意が必要である[16]。

さらに、改正個人情報保護法では、新しい概念として、要配慮個人情報が入ったが、これに当たる場合には、原則本人の同意なしに取得することができないこととされており（同法１７条）、オプトアウトによる提供もできないこととされているため（同法２３条２項）、要配慮個人情報を取り扱う業種における IoT の活用には、注意が必要となる。

個人情報保護法制に関しては、何が個人情報に当たるのか、要配慮個人上に当たるのかの判断が必ずしも容易とはいえず、所管する個人情報保護委員会において、事業者側の懸案を適切に吸い上げ、判断材料を提供していくことが必要となろう。

また、これら個人情報を含むデータを定型化し、技術上の流通可能性を高め、あるいは、本人の意思を反映しつつ流通を促進する観点から、PDS（Personal Data Store）、情報銀行などが検討されている。

このうち、PDS（Personal Data Store）とは、個人が自らのデータを蓄積・管理・活用（第三者への提供の制限を含む）するための仕組みであり[17]、情報銀行とは、個人からの預託により、個人に代わりデータを蓄積・管理・活用（第三者提供を含む）し、個人に便益を還元する事業者である[18]。

これらは、いずれも本人による第三者提供の同意を前提とした仕組みとして位置づけられており、このような制度が整備されることにより、これら情報の流通が促進されることが期待される。もっとも、情報銀行のような第三者に自身の個人情報を預けることについては、それにより生ずるリスクの分析が不十分で、法制度としての慎重な判断が必要なほか、これを躊躇する者がそれなりに出る可能性があり、まだ議論はスタートラインに立ったばかりといえるだろう。

14「データ流通環境整備検討会・AI、IoT 時代におけるデータ活用ワーキンググループ中間とりまとめ（案）」（以下、「AI、IoTWG 中間とりまとめ案」という。）P6＜http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/detakatsuyo_wg_dai9/siryou1.pdf＞。例えば、病院の場合、国立病院であれば、行政機関の保有する個人情報の保護に関する法律、私立病院であれば、個人情報保護法が適用法となる。関連情報について後述。

15　匿名加工の方法について、個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」＜http://www.ppc.go.jp/files/pdf/guidelines04.pdf＞、同「個人情報保護委員会事務局レポート：匿名加工　パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」参照＜http://www.ppc.go.jp/files/pdf/report_office.pdf＞。

16　なお、カメラ画像の取扱に関しては、ガイドラインがリリースされている（総務省・経済産業省・IoT 推進コンソーシアム「カメラ画像利活用ガイドブック」＜http://www.meti.go.jp/press/2016/01/20170131002/20170131002-1.pdf＞）

17　英国ビジネス・イノベーション・技術省「The midata Innovation Opportunity」＜https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262271/bis-13-1314-the_midata-innovation-opportunity-v2.pdf ＞にて記載

18　COCON（産業競争力懇談会）「IoT 時代におけるプライバシーとイノベーションの両立」にて提言

② AI にまつわる問題

AI ネットワーク化検討会議報告書 2016P34、37 では、法制度、権利利益に関するリスクとして、事故のリスク、犯罪のリスク、消費者等の権利利益に関するリスク、人間の尊厳と個人の自立に関するリスク、民主主義と統治機構に関するリスクが挙げられている。

このうち、事故のリスク、犯罪のリスク、消費者等の権利利益に関するリスクに関しては、IoT において、AI 技術を利用した場合でも、生じ得る問題であり、法的環境における課題でもある。

6）その他関連する法的環境について

① 各種業界における法的環境

ここでは、今回の調査対象となった各分野における法的環境を適示する。

まず、IoT において、各業界において利用する道具などが Things となった場合、各業法との抵触が問題となり得る。

例えば、畜産においては、と畜場の設置に関して、と畜場法があり、これにより、と畜場の設置の許可がなされているが、と畜場の衛生管理は、同法６条・同法施行規則３条により定められている。IoT を導入したからといって、それだけで問題となるわけではないが、IoT による設定ミスなどに気づかず、長期間放置するなどということがあれば、問題が生じ得ることになる。

医療・福祉分野に関しては、IoT のサービスや端末が医機法にいう医療機器に当たってしまう場合も生じ得るであろうし、その業務の性質上、個人情報保護法における要配慮個人情報を取り扱う可能性も、他の業界よりも多くなるものと考えられる。

また、福祉分野に関しては、入所している本人において、自身で完全な合意を行うことが難しいことも考えられ、その場合には、同人の法定代理人の許可を得る必要が出てくることも想定される。

なお、医療に関しては、データの流通の観点から、運営主体の違いにより、個人情報保護法制における適用法が異なり、取扱いも差異が出てしまうとの指摘があるが、これに関しては、設置主体の相違に関わらず医療情報を統一的な仕組みにより収集し、一体的に管理・匿名化を行い、利用につなげていく新たな基盤（「医療情報匿名加工・提供期間（仮称）」）に関する検討が進められているとのことである[19]。

② ドローン

ドローンに関しては、既に航空法の改正や、小型無人機等飛行禁止法により、飛行方法に関する規制は形成されてきている。

もっとも、ドローンと地表の所有権との法的関係は、未だ明確とはいえず、ドローン同士の事故、ドローンの人身事故などが生じた場合の法的処理に関しても、自動車事故のように、道路交通法規により細かなルールが決まっており、事例も豊富に存在するものと異なり、明確化には今後の事例の蓄積を必要とすることが予想されるところでもある。

また、航空法の下でのドローンの利用にはかなりの制限があり、ドローンの利用範囲の拡大に伴い、どのように法環境を整備するかさらに検討される可能性がある。

19　AI、IoTWG 中間とりまとめ案 P22

③ システム開発契約における諸問題

IoT においては、端末利用者、端末製造者、IoT システム・サービス提供者など、様々なプレイヤーが存在し、当事者が複数となるにつれて、法律関係も複雑化している。

また、従来のソフトウェアとしてのシステムだけの開発と異なり、希望するシステムを実現するためには、用途に合わせた端末の取捨選択や、端末とやり取りするデータの種類、内容、形式などを含め、様々な調整が必要となり、また、様々な業種において、様々な形態のサービスが利用されることになることから、利用する側の様々な専門性を十分に反映させる必要があり、これまで以上に関係者間での調整が必要となる。その意味では、プロジェクトマネジメント義務と協力義務の関係を含め、システム開発契約においては、さらに慎重な対応が求められるものと考えられる。

さらに、上記のような多数当事者の関係するサービスである以上、それぞれの役割分担、責任分担は重要であり、これを明確に取り決め、相互理解を深める必要があるといえるであろう[20]。

④ 保険制度

IoT と保険とのかかわりについては、２つの場面が考えられる。

一つは、IoT を利用した保険商品の開発、もう一つは、IoT のための保険商品の開発である。

前者に関しては、例えば、ヘルスケア関係の IoT では、端末から得られた本人の健康状態に関する情報を利用し、適切な保険商品を提供し、保険会社におけるリスクを低減させることで、合理的な条件での保険を提供するものである[21]。

後者に関しては、IoT の内容・用途が多様であり、そのリスクもそこまで明確ではないことから、これからのことと思われるが、現状でも、サイバー攻撃保険が IoT 機器に拡大されるなどの動きはある様子である[22]。

7）結語

以上みてきたように、IoT といっても、これまでの Internet、Things とは全く別の法律が直ちに必要になるわけではなく、現在ある法環境により、対処できる部分も多くある。

もっとも、それでは足りない部分や、現在の環境では円滑さを欠くものもあり、法制度を作った場合の影響なども考慮に入れつつ、今後も検討が行われるものと思われる。

また、法解釈についても、これからの蓄積が必要なものが多く、また分野が多岐にわたるため、個別の検討が必要となるだろう。

このように、IoT をめぐる法的環境は、未整備な部分が多いが、ある程度の法的環境が整っている領域もある。そのような領域では、その法的環境を最大限生かし、イノベーションを進展させていく必要があると思われる。

さらに、IoT においては、IT や ICT の延長として捉えられている向きもあるが、特に、物の動静に関して、情報セキュリティの観点だけでなく、安全性の観点からの考察も必要となる。この点については、いわゆる制御系の業界において蓄積されたノウハウを必要とする場面が多いに出てくるものと予想されるところである。

以上

20　参考として、IoT セキュリティガイドライン案 P.53

21　情報処理推進機構ニューヨークだより８月・八山幸司「米国における IoT（モノのインターネット）に関する取り組みの現状」P6 では、US の例として、「保険業界は、IoT によってコスト削減や業務効率化、保険加入者のリスク査定を向上できると考え、一部の保険会社は既に、IoT 機器を使った従量基盤保険（usage-based insurance:UBI）という商品を提供している。UBI では、IoT 機器を使って保険加入者の行動を追跡し、より安全またはより健康的な行動に対し、保険掛け金の割引や何らかの得点を提供するというものである」と報告されている。

22　日本経済新聞ウェブサイト 2017.01.25 記事「サイバー攻撃保険を拡充　ＩｏＴ機器対象に 損保各社、休業補償も」＜http://www.nikkei.com/article/DGXLASGC14H02_V20C17A1EE8000/＞