「第50回世界情報社会・電気通信日のつどい」記念講演より
IoT・AIの未来とセキュリティの課題
—これからのICTをどう進化させるか—

国立研究開発法人情報通信研究機構（NICT） 理事長　徳田（とくだ） 英幸（ひでゆき）

1. はじめに

「今、IoTで何が起きているか」、そのキーワードは「創発」である。あらゆる分野、特にIoTとはそれほど近くなかった方たちが、自分のビジネスとIoTを掛け合わせると新しい価値が生まれるのではないかと勇気づけられる、いわばイネーブラーとしてのICT技術の側面が認知され、社会全体で「創発」が起きている。実際、2015年10月に、総務省、経済産業省、民間と連携して、IoT推進コンソーシアムがスタートし、設立総会には約900社弱、現在では既に3,000社を超える方々が参加している。私は技術開発ワーキンググループ（スマートIoT推進フォーラム）の座長を仰せつかっている。

その中で、日本で初めてとなるIoTセキュリティガイドラインを作成した。今までより一桁も二桁も多くの機器がインターネットにつながるようになるのは、それ自体は素晴しいことだが、それらのデバイスや機器が踏み台にされて、攻撃する側に回ってしまうという事態が起きている。それを防ぐために、これからIoT機器をデザイン、製作する方たちの指針となるべきガイドラインを、方針、分析、設計、構築・接続、運用・保守、破棄といったライフサイクル全体にわたってまとめた。これが現在英語になって世界に向けて発信するベースとなっている。

ここでは、次の三部構成で話を進めたい。最初は、IoTサービスの事例、社会的・経済的インパクトについて。2番目は、こういう環境が私たちの身の回りに普遍的に存在するようになったときにどうなるか。一般の人たちが使いやすい形に技術を変えると同時に、社会的な仕組み、規制、制度などソーシャルイノベーションで社会を変えていかなければいけないという議論。そして3番目に、セキュリティの現状と課題についてである。

2. IoTサービス

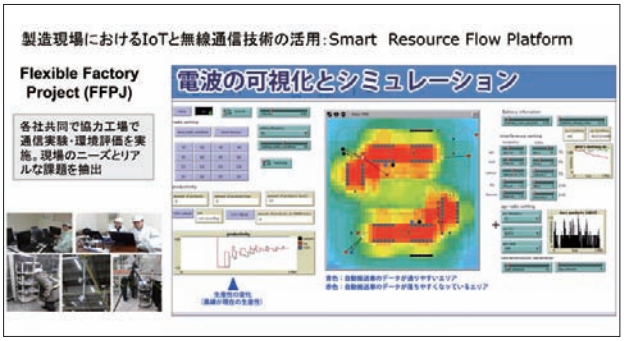
2.1　IoT化の加速

これまで単体でモノを売っていた会社が、売りきりではなく、全てがネットワークにつながるようになる。つながったプロダクトはそれを通じて様々なサービスが提供できるので、“Product as a Service”という進化が起きている。そして、product AがA service、BがB serviceになり、A、B serviceがコネクトされて新しいサービスができる。すなわち、“Everything as a Service”となり、あらゆるもののサービス化が加速している。これは新しい付加価値を作る上で一つの鍵になる言葉である。いくつか例を示す。

1つ目は「RainMachine」というスプリンクラー装置である。これは、自分の家の周囲1.6km四方の天気予報をインターネット上から取得して、予報の状況に応じて最適な水量を計算し、庭の芝生の水やりをする。カリフォルニアなどは、夏の家庭の水道水消費の70%は芝生に撒く修景用水なので、これを利用することによって節水が可能になる。

2つ目は、GEのデジタル・ツインという概念で、Industrial Internet of Thingsといわれているものである。GEはジェット機につなげるエンジンを売っているが、昔は、離陸、定常状態、着陸のそれぞれ数分間の3回分ぐらいしかデータをとっていなかったそうだ。これを1分間に1回、高精度でエンジンの状態について、温度、回転数等、あらゆるデータをとり、その飛行機のエンジンがどういう状況で動いているかを解析する。その上で、予防的なメンテナンスプログラムを組み込み、運行時はジェットエンジンの消費を最小に抑え、着陸時には次のフライトに向けてどういった予防的保守をすべきかの仕組みを作っている。このシステムを導入した航空会社では、年間4億円近い燃料費の節約になっていると言われている。

次に、NICTのFlexible Factory Project（**図1**参照）。実は、工場内に色々な機器やセンサーが無線で導入されることで、製品を運ぶ自動搬送車との通信パケットが落ちる不具合も起きており、そのホットスポットを赤く表示している。無線のセンサーがONになると、赤いゾーンが一気に増えてしまう。



■図1. Smart Factory：Flexible Factory Partner Alliance（by NICT）

無線なので作業をしている人たちには何が起きているかよくわからないが、それをシミュレーションで自動搬送機がどれくらい効率よく動いていないかをグラフでプロットして電波の状況を可視化し、異種の無線機器が工場内で混ざって使われる場合の動きの効率化を図ることができる。このSmart Resource Flow Platformという技術を我々の研究者たちがつくり、今、allianceができたところである。

もう一つは、日本自動車研究所がつくばで実際に走行したコネクテッド・カーの事例である（**図2**）。時速80kmで大きいトラックが3台、小さいトラックが1台、合計4台が4m間隔で走る。これによって車の渋滞が減るだけではなく、エネルギーの節約にもなる。自動走行に対して期待が大きい部分である。

さらに、データとサービスの連携はIoTの特徴である。自動車保険に入ると保険会社からODBポートⅡに差し込むセンサーやシガーソケットに差し込むようなデバイスが送られてくる。それで運行状況のデータをとり、安全運転をしているドライバーには保険費用を下げるというインセンティブを付けるサービスもある。日本の運送業界の場合、ドライバーの健康状態、運行状態の記録をとる運行管理用のプログラムがあるが、コネクテッド・カーのデータだけでサービスを考えるのではなく、そのデータと全く違うビジネスドメイン、この場合保険などを掛け合わせることにより、新しいサービスが生まれている。

その反面、悪い事象も起きている。車の「動く」「止まる」「曲がる」という基本機能が乗っ取られると非常に怖い状況になるが、BlackHat2015の会議でクライスラーのジープに対してペンシルベニアから攻撃者がハッキングした事例が報告された。

攻撃者はいろいろな形で既存のシステムを解析しているが、アメリカでは2016年11月にDMCA（Digital Millennium Copyright Act=デジタルミレニアム著作権法）を改定し、自分が所有している車やスマートテレビであれば、合法的にハッキングを行い、解析して中を見て良いとした。この法律によって、セキュリティ研究者のセキュリティがある程度担保される。日本では、研究者がどこかの車をハッキングして、それを一方的に発表すると威力業務妨害で、なぜ勝手にハッキングして公表したかという問題になり、セキュリティ研究者のセキュリティをどう担保するかが課題となっている。

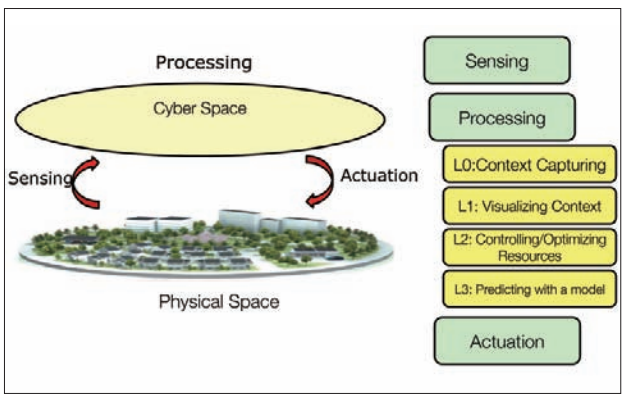
2.2　IoTとは?

IoTを、多くの新聞では「モノのインターネット」と解説しているが、物（オブジェクト）、人工物だけでなく、人や生きもの（creature）、あるいはデータ、ビジネスセグメントの違う人たちがデータを接続し合ったり、プロセスを接続させたり、まさにあらゆるモノがインターネットに接続され、情報を交換し、相互に利用される環境である。IoE（Internet of Everything）という言葉を使う人たちもいる。あらゆるモノとは、例えば位置情報、空間の情報で、サービスと接続することができる。それは『ドラえもん』の「どこでもスイッチ」や「どこでもドア」の技術に通じる。

IoTという言葉は十分に浸透したが、その中にCPS（Cyber-Physical System=サイバー・フィジカル・システム）がある（**図3**）。略称ではInternet of Controlled Things、制御されたモノたちということで、実際にサイバー・フィジカル・システムというのは、我々が住んでいる物理空間とサイバー空間が融合されて、それを股にかけて動いている、制御されるあらゆるモノたちである。例えば交通システムや、水の管理をするシステム、スマートグリッドなどのエネルギー系のシステムだが、そういうものはIoTというよりは、サイバー・フィジカル・システムと言われている。

サイバー・フィジカル・システムは、物理空間上からあるデー

■図2. Connected Car：自動運転＋コネクテッドサービス



■図3. サイバー・フィジカルシステムの視点

タをセンシングして取ってきて、それをサイバー空間上に持ち込み、処理をして、結果を物理空間上に戻す。例えば車の渋滞情報の場合は、車の流れをセンシングして、それを緩和するための信号機のリズムを変えて、その制御信号を物理空間上に戻す。戻した状態で再びセンシングをして、新たなロジックを立てるということで、この状況がくるくる回る。これを“共進化”といい、実際にいろいろなアプリケーションが作られている。

まず物理空間上でセンシングして、その後、レベル0として状況認識をする。どんな状況にあるかをまず認識して、それをレベル1のアプリケーションでは、科学技術的可視化をする。この可視化は、単なる見える化ではなく、例えば、電波がどこでcollision（衝突）が起きていて、不具合が起きているかが直感的に分かるようにヒートマップなどで表現することである。

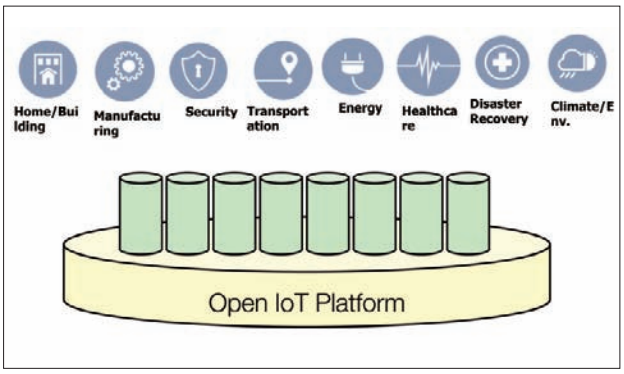
レベル2のアプリケーション群は、交通システムであれば、車の流れを最適化、最適制御や最適配置ができることである。最近では、“Digital Optimization”と言われている。

最後のレベル3は、予測するアプリケーションである。分かりやすい例では、天気予報で台風が24時間後にどこに到達するかというのがある。今、NICTがやっている事例で、次世代のPhased Array Weather Radarとして埼玉大学の屋上に特別なマルチパラメーター・フェーズドアレイ気象センサーが置いてあり、三次元の降水分布の予報を計算し、可視化している。昔のパラボラアンテナ型レーダーはぐるっと回って、雲の状況を解析するのに5〜10分かかったが、最新のレーダーでは10〜30秒のあいだにスキャンすることができ、スムーズに三次元的に雷雲がどう発達していくか可視化できる。これは東京オリンピックの2020年には十分活躍してくれると期待しているアプリだ。

2.3　IoTエコシステムの構築

このようにリラックスしたIoTと、制御を対象にしたサイバー・フィジカル・システムを全部ひっくるめてIoTになっているが、エコシステムの構築、すなわち、いろいろな業界を飛び越えて、様々なデータが流通できるオープンなIoTプラットフォームを作ることが大事である。エネルギーの中はかなりデータが流通するようになったが、エネルギーのデータをセキュリティ会社に流したり、製造業に流したりするなど、ホームビルディングの環境をエネルギービジネスとつなげたいわけである（**図4**）。

データフォーマットやデータの意味を表現しているものをメタデータというが、通常はメタデータをきちんと付けた形でデータが流通していないので、異業種間ではなかなかデータの共有ができない。同じように、異業種間でデータマーケットプレイスがうまくいかない。例えば、大手町で働いている若い女性が、何色の、どういう服を買っているかのデータが欲しいという人と、それを売りたい人をマッチングさせるような場所が必要になってくる。では、どのように買いたい情報を表現して、売りたい情報を表現するとマッチングサービスがデータマーケットプレイスでうまくいくかが問題である。異業種間でのデータのマッチングは非常にチャレンジングな部分だが、IoT、AIのビジネスモデルや、人材の問題も、エコシステムを作る上では大事である。



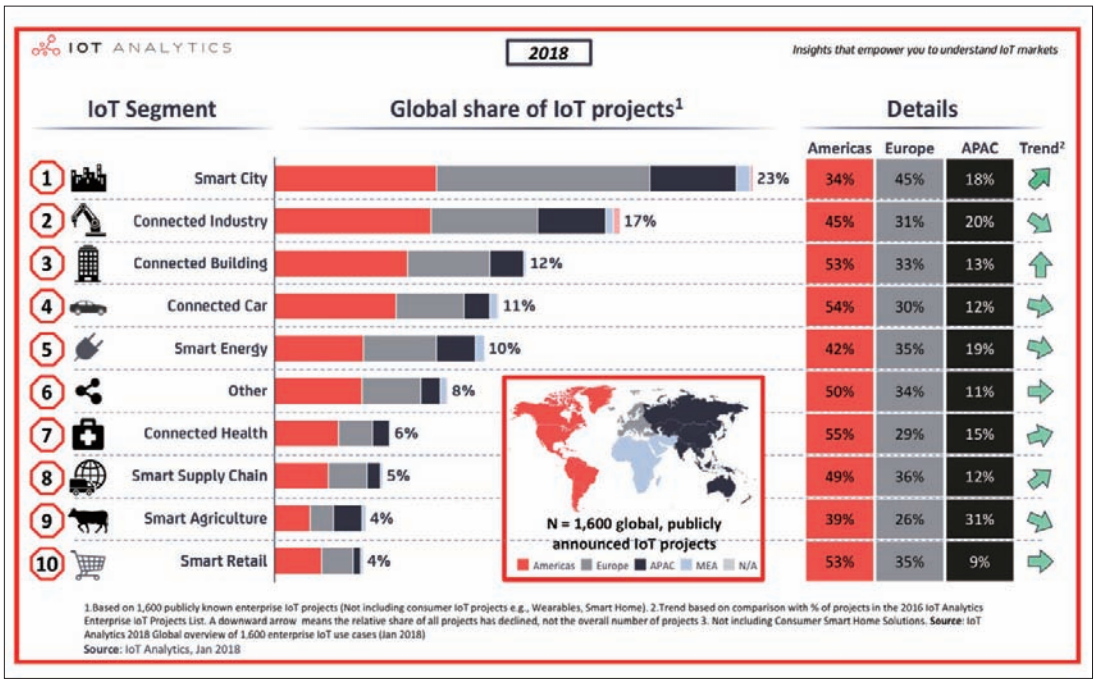
■図4. オープンIoTプラットフォーム
サイロとプラットフォームの統合

一方、世界を見るとどうか。ドイツのIoT Analitics.comという会社でIoTの動きを追いかけて分析しているが、2016年はIndustrial Internet of Thingsがプロジェクトの数では一番多かった。2018年は、Smart cityが第1位で、さらに伸びている。2番目がConnected Industry、3番目がSmart Buildingとなっていて、Connected Carが4番目。年々、多少ランキングは違うが、トップ5くらいまでは同じである（**図5**）。

2.4　IoEの経済的インパクト

IoEの経済的なインパクトは、ドイツの解析会社の分析によると、ドイツの2016年現在のGDPは3.6兆ドルだそうだが、2023年にはそれを超えるだろうと予測されている。あと5年もすると莫大なビジネスセグメントが生まれるのではないか。

つまり、IoTは、新産業の創出のイネーブラーとなるだろう。ヒト・モノ・プロセス・データなどの接続によるイノベーションの創出ができるし、サイバーフィジカル空間のエンパワーメントをしてくれる。その一方で、接続されたサービスによるイノベーションとともに、セキュリティ攻撃が多様化してきている悪い面もある。



■図5. IoT/IoEのアプリケーション分野（by IoT Analytics.com, Jan. 2018）

さらに重要な問題として、認証基準やセキュリティプロトコル、ソフトウェアの検証などによる新たな参入障壁の発生も考えられる。例えば、ある国の車が世界各国で売られている場合に、貴国の車は自動運転のソフトウェアが未検証なので、我が国においてはコネクテッドサービスはONにできないといったことが起こり得る状況になってきている。

これらIoTの進化は何が牽引していくかというと、つながるメリット、コストメリット、ネットワーク化のメリット、スケール化のメリット、エネルギーメリット等々あるが、今日のメッセージの一つは、“つながるメリット”が大きくなる反面、ほぼそれに比例して“つながるリスク”も大きくなってきているということである。

3. IoT・AI環境の未来

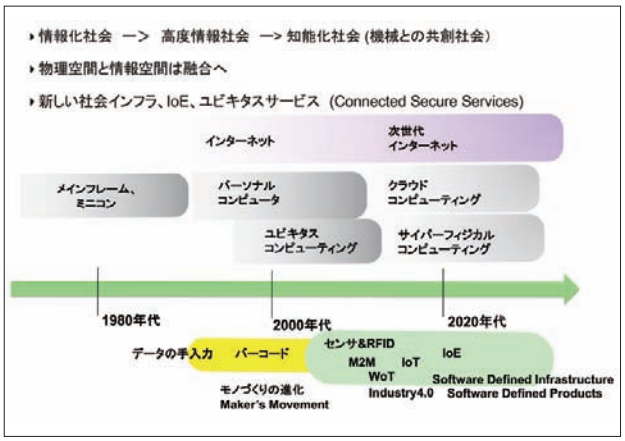
3.1 SFC25周年デモとシンギュラリティ

慶應義塾大学で2015年にIoT・AI環境の未来についてデモンストレーションを行った。お年寄りが個人用ロボットと住んでいて、病院にリハビリに行くのだが、リハビリを忘れているという設定で実施し、3つの課題について検証した。1つ目は、ロボットと人間のコミュニケーションを通じて、お年寄りのQOLを向上することができるか。2つ目は、ロボットどうしでコミュニケーション、あるいはソフトウェアエージェント間での通信がスムーズにいくか。3つ目は、お年寄りのために自動運転のロボットタクシーを呼び出し、人を介さずにロボットどうしで物事を処理できるか。このロボット・ツー・ロボットタクシーのコネクテッドサービスも、まだプロトコルが確立されていない。自動運転に関しては、慶應湘南藤沢の大前先生の研究室で10年ほど研究されているが、このデモンストレーションを通じて大きな課題が見えてきた。

では、2020年から2030年にどういう未来社会になるか。一言で言うと、機械と人間が共創する社会になるだろうと考えられている。これまでは人と人のコラボレーションが進んだが、これからは、人と機械もCo-creation、Co-designする世界になっていき、あらゆるものがソフトウェアによってコントロールされるものになっていくのではないか（図6）。

我々もNICTのスポンサーシップで日欧プロジェクトを立ち上げ、クラウドとIoTの融合によるスマートなまちづくりに取り組んでいる。その一例として行った藤沢市では、ごみ収集車にハードウェアのセンサーやカメラを付けたり、市の職員のスマートフォンから参加型センシングでデータをとったり、Webのデータを仮想センサーとして投稿できるように変えることによって、いろいろなサービスをつくって実験をした（図7）。

藤沢市の場合、5年に1度、道路の白線がどのくらいかすれているかを人が目視し、マーキングして修理していた。そこで、毎日個別集配しているごみ収集車のカメラで撮影したものを学習させて、白線のかすれ度合いをディープ・ラーニングで確率を出し、高いところをマーキングするという手法を取



■図6. 2020年ー2030年の社会イメージ

■図8. ゴミ収集車のカメラによる白線かすれ自動検出

■図7. アプリケーション（藤沢市の例）

り入れた（図8）。また、“ピギーバック方式”と呼んでいるが、普通に働いている方たちの車にカメラを付けてデータをとる。これによって白線のかすれ以外にも、落書き、不法投棄のごみ、道路標識の不具合等々を、人手をかけずにマーキングできるようになった。さらにAIとIoTを掛け合わせることによって、多様な新しいサービスができてきている。

3.2 IoT・AI環境の光と影

今あるAIはブラックボックスAIと言われているが、何か不具合が起きたときに説明可能なAIに変えようとしている。さらに、問題なのは、学習するデータがいかにフェアな、バイアスのないデータかを担保しなければいけない。そして、どのような形でデータを整理するかという問題だ。例えばNICTのユニバーサルコミュニケーション研究所では、同時通訳のプロトタイプによる言語の壁の解消に取り組んでいる。さらには、我々が年を取って寝たきりになり、うまくしゃべれなくなったときに、脳の活動からわれわれが何を考えているか、何を見ているかを逆変換する（ブレインモデルに基づくデコーディングという技術）研究も行っている。

このようにいろいろ画期的な技術が生みだされる一方で、

IoTの影の部分として、自動運転の車の事故が発生した。一番ショッキングだったのは、自転車で道路を渡っている女性にボルボの車に自動運転用のセンサーが付いたUberの試験走行車がぶつかり、死亡させた事故である。

これについては多くの研究者が分析をしているが、Mobileyeの専門家が公開された事故当時の映像を分析したところ、被害者を衝突1秒前に検知できているので、何らかの形で衝突は避けられたはずだと検証している。飛行機の場合は、ブラックボックスがあり、海に墜落した場合でもそれを回収するとデータが取れるが、今回のように説明がつかない障害が起きたときには、ログデータ等が担保されているべきである。さらに、何十万時間のテストをしているときに自動運転のトラブルが何回起きたかについて、カリフォルニア州の運輸省のホームページで記録が報告されているが、そういう制度的な枠組みを改良することと、説明可能なロジックにシステム自体を持っていこうという動きが加速している。これができなければ、どれほどの大量の実験をして、どこまでのテストが済んだら一般走行を許すのかといった検討をするところまではいかないということである。

野村総研は、このように人と機械が共創する時代になったときに、いかに人間の仕事が奪われていくかを分析し、「日本におけるコンピューター化と仕事の未来」にまとめた。そこでは日本の労働人口の約49%が、技術的には人工知能やロボット等により代替される可能性が高いとしている。例えば、電車の運転手、経理事務員、検針員、一般事務員等である。一方、芸術、歴史学・考古学、哲学・神学等、抽象的な概念を整理・創出するための知識が要求される職業、あるいはネゴシエーション、サービス指向性が求められる職業は代替が難しいのではないかとされているが、この視点は、仕事・タスク中心に世の中を見ている。

ところが、アメリカにはInnovation 4 Jobs（i4j）という動きがある。ノードフォース氏は、ITと人工知能は労働者によって意味のある新しい雇用を創出するツールとみなすべきであり、今の企業はタスク中心で経済を考えているので、同じタスクならばどんどん機械に置き換えればいいと考えているが、もっと人間の価値に焦点を当てた、“人”を中心とした経済を考えるべきであるというメッセージを発信している。AIがすぐに仕事を奪うといった敵対的な考え方より、企業の総資産は働く人の価値の総和であるという考え方を持つべきであるとしている。

2045年以降の社会イメージは、これまで体外で起きていたICT革命が体の中でも起きてきて、人間の記憶や存在が機械と融合した社会になるだろうとされている。singularity（特異点）という言葉があるが、私は2006年に特異点論者のレイ・カーツワイル氏にインタビューをした。彼は、人間と機械、物理的な現実とバーチャルリアリティとの間には全く区別が存在しなくなり、我々の記憶、意思決定をするロジックも、全て体の外に出せると言っている。これに対し、私が私であるというのは、物理的に触って、自分の感覚がフィードバックされてこそ、はじめて私だとわかるのだと言う人たちもいる。どのような社会のかたちにすべきかは、我々が真摯に考えなければいけない問題である。

4. IoTセキュリティの課題

4.1 IoT環境の脅威とリスク

IoT化が進んだ社会では、我々にとってますますセキュリティの課題が重要になってくる。セキュリティの課題は、国レベル、企業・組織レベル、コミュニティレベル、個人レベル等、いろいろな場面で問題になる。かつ技術的な側面と制度的な側面がある。さらにIoTのレベルで言うと、スマートフォンやウェアラブルデバイスのような身近にあるデバイス、ネットワーク、クラウド等の上に作られているコネクテッドサービス、いろいろなレイヤーで攻撃は起こる。

この状況に対して、内閣官房のNISC（内閣サイバーセキュリティセンター）では、2015年に新たなサイバーセキュリティ戦略として「安全なIoT活用による新産業創出」を提示している。キーワードとして、「後手から先手へ」「受動から主導へ」「サイバー空間から融合空間へ」を掲げ、我が国ではかなり早くからこの危機について議論を始めていた。

一方、セキュリティの問題点は、非対称性問題である。攻撃側のコストが守備側のコストより圧倒的に少なくて済むのに対し、人数では攻撃側が守備側より圧倒的に多い。ダークサイドでのビジネスマーケットが既にできているし、さらに、攻撃側のスピードは守備側のスピードより速く、ここは侵入できると分かると、その情報はまたたく間に攻撃者側に拡散する。コスト、人数、スピード面での非対称性の流れをどう変えたらゲームチェンジができるかが課題だ。

IoTの中では、これから新たに付加価値を付けたサービスを作る場合は、ライフサイクルの企画設計から、詳細設計、実装、接続、運用、保守、破棄全てにわたってSecurity by DesignやPrivacy by Designなど、あらゆるフェーズでのセキュリティ、プライバシーを最初から考えるプロセスに変える必要があるのではないか。同時に、消費者側のIoTリテラシーも変えなければいけないし、いわゆるディフェンダーズ・

ムーブメント、我々がおかしいと感づいたときに何らかの形でレポーティングできるようなものが必要になってくる。

4.2　これからの課題

管理の行き届いていない、一度設置したらほとんど手をかけないIoTデバイスを“のらIoT”デバイスと呼んでいるが、これらへの攻撃が増えていることは脅威である。2016年に発表された横浜国立大学の吉岡先生のデータでは、約60万台のデバイスがものすごい勢いで侵入攻撃されて、踏み台にされたということだ。

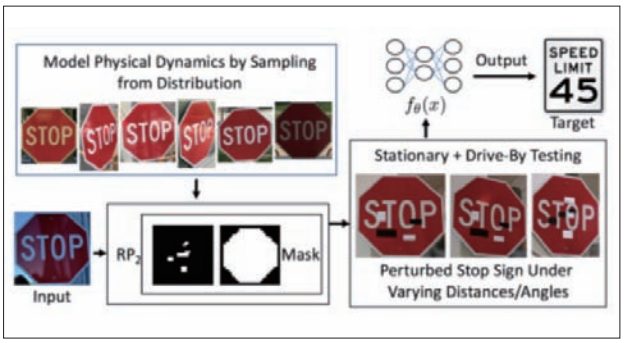
特に“のらIoT”デバイスで対象となるシステムを見ていくと、電力、電車、ATM、スマートメータなどは、SIP：「要インフラ等におけるサイバーセキュリティの確保」ということでプロジェクトが動いているが、IoT/ホームゲートウェイ、ホームエネルギー・マネジメント・システム、スマート家電、スマートスピーカー、スマート健康機器、ロボットなど、一度設置すると管理が行き届いていないものが踏み台にされている。

実際、NICTのセキュリティチームが攻撃対象をモニタリングしてみると、状況が大きく変わってきていることが分かった。昔はサーバー系の攻撃が多かったが、今はIoT機器のWebカメラなどへの攻撃が約50%を占めている。マルウェアが感染した例では、極度にひどかったケースでは1日に7億パケットのIoTスキャンがされていて、踏み台を見つけて、それを捕まえると、また攻撃に行くという形になっている。

IoTセキュリティガイドラインももちろん大事だが、それからさらに一歩進めて、国内・国外を巻き込んだ形の標準化が必要であるし、IoTセキュリティマークを導入し、これらが付いた機器が浸透することが望ましいと思っている。

AIへの攻撃も非常に緻密になってきており、ミシガン大学のチームが作成した2018年6月発表の論文「敵対的機械学習」で、自動運転車への標識を認識するアルゴリズムに対する攻撃事例が報告されている。ストップサインを認識するアルゴリズム、機械学習で学んだものに対して、ストップサインにあるノイズを故意に入れたところ、機械学習のアルゴリズムがスピードリミット45マイルの標識と誤認識してしまう。これは理論的には分かっていたのだが、実際に車を走らせて何マイルで走っている状態でも誤認させることが可能だということを実証した（**図9**）。

ITS環境下でも同じように、実際には物体がないのに、あたかもそこに何か物があるかのようにして、急ブレーキをかけさせるといった、そういう高度な攻撃が可能になってきている。



■図9. 自動運転車のストップサイン認識への攻撃事例
（by K. Eykholt et al., to appear CVPR2018）

これらのことからも分かるように、セキュリティの人材育成については、産官学連携で拡大していかなければ、我々の未来の社会の形が曲がったものになってしまうおそれがある。NICTでは総務省と協力してナショナルサイバートレーニングセンターを2017年4月からスタートしている。内容としては、国の行政機関、地方自治体、重要インフラ関係者に年間3,000名ほど、CYDERプログラムでNICTの演習に関わっていただき、マルウェアに感染した機械がどのくらいあるか、どう対処していくかについて体験学習をしていただいている。また、Cyber Colosseoでは、東京オリンピックに向けてセキュリティを担保する人たちのトレーニングを行っている。さらに、SecHack365では、25歳以下の人たち約50名を1年間かけて、将来のホワイトハッカー、セキュリティエンジニアに育てるための育成プログラムを実施している。

5. おわりに

私たちがどういう形の未来社会をつくるかは、私たちが技術、制度を設計しているわけであるから、Security by DesignやPrivacy by Designと同じように、Japan by Design、Future Society by Designということで、みんなの知恵で、より安全・安心なIoT・AI社会に向けて進んでいかなければいけない。サイバー・フィジカル空間ということで、我々の生活環境は拡大されたが、それらの安全性を担保する仕組みを作っていかなければいけないと思っている。

※本記事は2018年5月17日開催の「第50回世界情報社会・電気通信日のつどい」での講演をリライトしたものです。

（責任編集：日本ITU協会）