



cutting through complexity

モノの インターネット

私たちはその潜在力を
全面的に受け入れるべきか

Cyber Insights Magazineへ ようこそ

本誌では、モノのインターネット時代の幕開けと、それがプライバシー、ビジネス、社会全般にもたらすと思われる影響について、KPMGのサイバーセキュリティ専門家が、対立する見方も交え、それぞれの見解を展開します。チーム内でも意見が分かれ、論議となるテーマですが、私たちは無理にコンセンサスを形成するのではなく、このテーマの専門家たちが自由に意見を出し合えるような場を用意しました。

ここに掲載されている意見は各筆者のものであり、必ずしもKPMGの見解を表すものではありません。

サイバーセキュリティの将来の展望と、デジタル時代において英国がどのように変化していくかに関するさらに詳しい情報は、www.kpmgslant.co.ukをご覧ください。

本冊子は、KPMG英国が2015年に発行した“THE INTERNET OF THINGS –SHOULD WE EMBRACE ITS FULL POTENTIAL?”を翻訳したものです。翻訳と英語原文間に齟齬がある場合には、当該英語原文が優先するものとします。

目次

モノのインターネットはビジネスの世界を変える	02
モノのインターネット – 普及までのタイムスケール	04
モノのインターネットによって個人のプライバシーは過去のものに	06
モノのインターネットが医療を根底から改善する	08
私たちは自覚がないまま機械の世界へ誘い込まれるのか	10
モノのインターネットは人間性を窒息させる網である	14
モノのインターネットは我々を暗黒の未来へ駆り立てる	16
ロボットの黙示が迫る	18
モノのインターネットは社会格差を広げる危険がある	20
私たちは自主性を保てるか	22



ナレーター：KEN HALL

KPMGのサイバーセキュリティ担当パートナー。30年以上にわたるITコンサルティングとセキュリティの経験を持ち、これまでに金融、メディア、電気通信、エネルギー、公益事業など、さまざまなセクターを担当。ヨーロッパにおけるSACのサイバーセキュリティ事業の立ち上げや、Wiproのグローバルサイバーコンサルティング事業の創設・運営に携わる。

モノのインターネット (IoT : Internet of Things) は、インターネットの誕生と同様に社会に大きな変革を起こすことが見込まれます。まだすべてのテクノロジーが整ったわけではありませんが、その兆しは明白です。IoTの実現は間近です。では、IoTとは厳密に何のことでしょうか。

IoTとは、多数のデバイスがインターネットと接続したり、相互に接続したりすることです。スマートテレビやスマートカーなどの明白なもの以外にも、認識機能が必要であるとは誰も考えていなかったデバイスにまでセンサーが組み込まれるようになり、ビッグデータ時代の幕開けを告げるでしょう。これら一連のデータとその分析が結びつくことで、今後インテリジェントシステムは大きく進化すると思われます。

間違いなく、それ以上に重要な問いは、これが私たちにとってどのような意味があるのかということです。私は同僚とともに、このテクノロジーがビジネスに与えるであろう影響と、いくつかの潜在的な機会や危険について調べています。本誌掲載の各記事は意見にすぎず、今後の道しるべとなるものはありますが、誰にも未来はわかりません。ポジティブに捉える者もいれば、厳しい未来を予想する者もありますが、備えあれば憂いなしです。

このテーマについて論じる前に、Anthony HessがIoTについてもう少し詳しく説明し、ビジネス界に与えるであろう影響を検証します。

“

モノのインターネットは、インターネットの誕生と同様に社会に大きな変革を起こすことが見込まれます”

”

© 2015 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

モノのインターネットは ビジネスの世界を変える

IoTについては、誇張されているとはいえないかもしれませんが、やがてビジネスを変革させるような影響力を持つでしょう。テクノロジーが広く採用されるには、予想よりも時間がかかるのが常ですが、次々に進化を重ねるうちに、以前とは全く違ったものが生まれます。

IoTによって巨万の富を築くテクノロジーの先駆者が生まれるでしょう。ビル・ゲイツ、スティーブ・ジョブズ、カルロス・スリムといったコンピューター業界や電気通信業界の大物に並ぶ人物が現れるはず。それどころか、より少ない人材でより多くの能力を活かすことができるようになるため、一層富が集中するでしょう。早い段階で新しい市場に迅速かつ低コストで参入し、巨大なネットワーク効果により市場を独占してしまい、他社の参入に対する障壁を築くことができる可能性はさらに高まります。早期参入者が独自の標準技術確立し、他者にその技術の採用を強いることができるようになるでしょう。ただし、政府のオープンスタンダードに対する支持によって、この傾向が緩和される可能性があります。

小規模企業でも、短期間にスケールアップできる、高度に自動化された製品やソリューションを開発することで、大きな収益をあげることができるようになるでしょう。今のWhatsAppのような企業を考えてみてください。ごく少数の小規模企業が多額の利益を得ています。IoTが軌道に乗れば、このような例が多数現れるでしょう。

あらゆる企業がIoTの影響を受けると思われますが、最初にB2C（企業と消費者間の商取引）企業においてその効果が現れるでしょう。消費者は早いペースで新しいテクノロジーを採り入れるため、一般消費者向けの企業はそれに追いつ

つかなければなりません。テクノロジー企業が当然先頭に立つでしょうが、鉄道などのB2Cセクターも短期間でキャッチアップする必要があるでしょう。

ここ数十年、テクノロジーの変革が波状的に起こっています。巨大なサーバールームに据え付けられた初期のコンピューターからマシンの小型化が進み、デスクトップコンピューターが生まれました。次の波は、これらのPCを相互に接続し、インターネットに接続することでした。現在、この2つのトレンドが合わさって、次の大きな波であるIoTが生まれようとしています。



モノのインターネットによって、巨万の富を築くテクノロジーの先駆者が生まれるでしょう



今後、自動化の拡大は避けられません。これまでの波と同様に、このようなことが起きるのは、進取の気性に富む技術者が実現可能であると信じ、クレバーなビジネスマンがそこに利益を見い出すからです。「コンピューター」とは無縁だった物体がコンピューターになり、ネットにつながり、データを処理するようになるでしょう。

卓上電話を考えてみましょう。かつて固定電話は独自のネットワークにつながり、デジタル機能は皆無でした。今日の電話は、データ処理機能を持たないハードウェアから、ハードウェア上で動くソフトウェアへと変化し、多くの人は仮定の固定電話をどこへでも持ち歩いています。

職場でも自宅でもネットにつながるモノが増えるに従い、これらのシンプルなシステムから巨大なデータベースに流れるデータが増加し、そこから相関関係の発見や意思決定のサポートが行われるようになるでしょう。これにより、人間が介入する必要性は必然的に減少していきます。かつてはデータを分析して上司にレポートを送るのは下位の管理者の仕事でしたが、将来はテクノロジーがその仕事を担うようになるため、人の介入は必要なくなります。

店舗内のどこにいるかに応じてスマートフォンにメッセージが送信されてくるiBeaconのようなハイパーローカライゼーションも進んでいくでしょう。顧客の習慣や支出パターンに関するあらゆる情報が小売店や消費財メーカーに送られ、マーケティング担当者が意思決定せずとも、テクノロジーがマーケティングに関する意思決定を下せるようになるでしょう。つまり、テクノロジーによって人材やバックオフィスに対する要件も変化するのです。

B2B（企業間取引）企業にも大きな影響が生じるでしょう。バイヤーとサプライヤーの力学が変化し、例えば、ある商品の在庫が少なくなると、デバイス同士が自動的に情報をやりとりするようになるでしょう。注文の追跡、供給される部品や材料の品質と性能の分析などについても自動化が進むでしょう。

企業のPCがネットワークに接続されたことによる大きな変化の1つが、管理構造のフラット化です。これはIoTでも続くと思われます。事務系中間管理職の職務の多くが消滅するでしょう。多くの現場管理者の職務も、この30年以上にブルーカラーの仕事に影響を与えてきたトレンドを追うことになるでしょう。

人材のニーズは変化します。サイバーセキュリティ専門家、システムアーキテクト、プロジェクトマネジャーなど、スキルの高いテクノロジーワーカーが必要とされます。今日の平均的な労働者が1970年代に比べて高いITリテラシーを必要とするのと同様に、すべての人がさらに高度なITリテラシーを身につける必要が出てくるでしょう。

コンサルタントや会計士などのサービス産業にも影響が及ぶと思われます。情報フローと分析の自動化が進めば、人間の創造性や判断力を必要としない業務は置き換え可能になるでしょう。こうした業務に携わっている人たちは、自動で生み出される分析結果を利用して、価値ある知見を提供するための新たな方法を考案する必要があるでしょう。

IoTは、サポートスタッフに対する企業のニーズにも影響を与えます。警備員、ケータリングスタッフ、清掃員などは、新しいテクノロジーによって職務が自動化されれば必要人数が減少していくでしょう。

IoTは、ビジネスのあらゆる分野に幅広く多大な影響を与えます。今後数十年で風景は全く違ったものになるでしょう。

“

今日の平均的な労働者が1970年代に比べて高いITリテラシーを必要とするのと同様に、すべての人がさらに高度なITリテラシーを身につける必要が出てくるでしょう

”



筆者：ANTHONY HESS

KPMGサイバーセキュリティ事業のシニアマネジャー。サイバー保険業務とサイバーインシデント対応業務のリーダー。2012年渡英し、KPMGに入社。以前は米国の大手軍需企業Raytheonにおいてエンタープライズアーキテクチャの構築に注力。

IoTがビジネスに多大な影響を与え、テクノロジーについていける者に重要な機会を提供することは間違いありません。この不可欠なテクノロジーの発展は加速していますが、スミスの有名な歌詞を引用するなら、「今にも、っていつ?」。Ben RamdunyがIoT到来のタイムラインを探ります。

モノのインターネット ー 普及までのタイムスケール

現在、実際にインターネットに接続して利用されているデバイスには、スマートフォン、自動車、ノートPC、テレビなどがあります。私にとってIoTとは、まだインターネットに接続されていないもの（例えば、靴、カーペット、電球など）をネットにつなげ、インテリジェントネットワークに無数のモノがあるという状況の中で、それらの用途を見つけていくことです。

私が心に描くIoTは、今から10年後には本格的に稼働し始めるでしょう。ビッグデータを収集し、パーソナライズされた広告を提供するために利用者のデータにアクセスしたいと考える企業が主導し、複数のデバイスが相互接続され、2035年にはあらゆる日常生活にそのような機能が完全に埋め込まれるでしょう。

アーリーアダプターはスマートガジェットを入手するために割高な価格を支払わなければならないため、最初にIoTを利用するのはお金に余裕のある人に限られるでしょう。持てる者と持たざる者とに分かれることになりそうですが、これが大きな問題になるとは思いません。IoTは具体的な何かを与えてくれるものではありません。生活必需品というより、あればいいといった類のものです。スマートフォンで点灯できる照明装置がなければ、スイッチを使えばいいのです。

しかし、やがてテクノロジーコストは低下します。薄型テレビは15年前にはほとんどの人にとって手の届かない商品でしたが、今やスーパーマーケットでは数百ドルで販売されており、テクノロジー企業は2020年までにIoT対応テレビを販売すると発表しています。データ収集会社や広告主も、商品・サービスのターゲット層を拡大しようと、あらゆる人にこうした商品を普及させることに関心を寄せるようになるでしょう。テクノロジーコストの低減が進み、少しの追加コストだけでセンサーを組み込んだデバイスを製造できるようになるでしょう。徐々に、どこにでもIoTデバイスがある世の中になるでしょう。



テクノロジーコストの低減が進み、少しの追加コストだけでセンサーを組み込んだデバイスを製造できるようになるでしょう



“

このテクノロジーがなくても十分に生活できますが、スマートフォンがそうであるように、一度体験してしまうとそれのない生活には戻りたくないと思うでしょう ”

”

デバイスのつながり方も進化すると思います。中央に接続するのではなく、デバイス同士がリンクし、各種センサーからデータの流れが生じるようになります。このデータをインテリジェントアプリケーションがリンクし、相互参照することによって、IoTは自宅でも職場でも本当の変化を起こすことができるのです。

例えば、電球ソケットにサウンドモニターを取り付けると、言い争う声を認識してムード照明を調節し、住人を落ち着かせるといったことができるようになります。同様に、カーペットがドア、照明、暖房装置と通信し、点灯や消灯を行ったり、部屋から部屋へ人が移動するのに合わせて暖房する場所を変えていくことも可能です。このテクノロジーがなくても十分に生活できますが、スマートフォンがそうであるように、一度体験してしまうとそれのない生活には戻りたくないと思うでしょう。

すでに暖房システムとリンクしてリモートコントロールできるデバイスが生まれ、ボイラー修理の必要性をオーナーが気づくより前にガス会社へ知らせてくれる、スマート修理サービスのトライアル運用も始まっています。これらの動向から見て、テクノロジーに精通した家庭では、あと5年ほどでデバイス同士がつながった時代が到来するでしょう。

ワイヤレス技術とセンサー技術の進化によって、照明スイッチ、ペンなどのスマートガジェットのコストは軽減されます。このようなデバイスには、最初は大きくて実用的な用途はないように見えますが、アーリーアダプターにとっては特別な意味を持つのです。一方で、スイッチを切り忘れるとリモートで知らせてくれるアイロンなど、用途が明確なスマートデバイスに対する需要も生まれるでしょう。メーカーはこれまでと同じように、利益が得られるのであれば商品を作るでしょう。



筆者：BEN RAMDUNY

2010年入社。KPMG情報保護チームのエンタープライズセキュリティアーキテクト。多種多様な業種・規模のクライアントを担当し、システムをサイバー攻撃から保護するための支援を行っている。ネットワークセキュリティとITコンシューマライゼーションが専門。過去には、オリンピックのITセキュリティプロジェクトに参加した経験や、富士通で政府向けの大型アウトソーシング契約のネットワークアーキテクチャを担当した経験を持つ。

新しいデータ収集・分析の時代には、プライバシーの概念も新しくなります。私たちはすでにオンラインショップ、銀行などの企業に、サービスと引き換えに個人情報を提供しています。この傾向は、デバイスが私たちの健康、移動、購買パターン、視聴の嗜好など、ありとあらゆる情報を収集するようになるIoTによって、さらに拡大するでしょう。顧客に関する情報には価値があり、現在市場で売買されています。大量のデータが作成・収集されている現状において、プライバシーとは何かということについて、Milda Petraityteが問いかけます。

モノのインターネットによって 個人のプライバシーは 過去のものに

これから私たちはプライバシーの少ない生活に慣れなくてはなりません。IoTの恩恵を受けようと思うなら、個人情報を提供することが当たり前にならざるを得ないからです。

あまり多くの情報を簡単に提供することには注意が必要ですが、インターネット検索にフィルターを適用するのと同じように、詳しい情報を提供すればするほど優れたサービスを受けられるようになるでしょう。スマート冷蔵庫に庫内の追跡を許可しなければ、牛乳が少なくなっていることをあなたに知らせることはできません。無脂肪乳が好きなことを伝えておかなければ、スーパーマーケットは適切な商品を用意できません。



こうした機微データをどのように保護し、
悪用を防ぐのかという疑問が生じます



このような動きは、スマートテクノロジーの到来と同時にすでに始まっています。例えば、テレビが各個人にふさわしい広告や、サービス、内容を提供するために誕生日をたずねたり、場合によっては子どもの誕生日まで入力させるといったことが行われています。

今や多くの人々が、依然として個人情報が大きな価値を持つ市場で、それがどのような結果を生むか考えずに、気軽に個人情報を提供しています。

IoTは私たちの生活を根本から変える可能性を秘めているものの、派手な宣伝もなければ、メディアがこぞって注目することもないでしょう。むしろ少しずつ生活に入り込み、相互接続されたデバイスが私たちのデータを集め始めるでしょう。バックグラウンドで計算処理が行われ、私たちの暮らしを楽ししてくれる特別あつらえのサービスが提供されるでしょう。

収集される個人情報の性質も変化すると思われます。誕生日や暗証番号といった特別なものではなく、日常生活の些細なことが収集されるようになります。使っている歯磨き粉の種類、睡眠パターン、好きなオレンジジュースのブランドなどです。多くの人がこれらの情報を気軽に提供し、それと引き換えに、例えば、自動作成された買い物リストや、寝ている間に位置調節してくれる枕やベッドなどのサービスを受けるようになるでしょう。

心拍数やコレステロール値などの健康指標を提供するウェアラブルデバイスは、それと引き換えに特定の治療法や医療保険の割引などのサービスを提供する機会を企業にもたらすでしょう。慢性疾患の患者をモニターすることで、いざという時に即座に対応できるようにになります。しかし、こうした機微データをどのように保護し、悪用を防ぐのかという疑問が生じます。

テクノロジーは急激に進化しています。Ciscoの2014年の予想では、インターネットに接続されるデバイスの数は、2013年の100億台から2020年には約500億台に膨れ上がるとされています¹。今後生み出されて処理されていくであろう膨大なデータ量を踏まえれば、今日私たちが考えるようなデータ保護は意味がなくなるものと思われます。データの保護を試みるためのあらゆるポリシーを備えることは可能であるものの、数が多すぎるため、そのすべてを追跡することはほぼ不可能でしょう。

従来よりも進んだデータ保護のポリシーや技術を考案すれば個人のプライバシーを保護できるという議論もありますが、個人情報の使われ方を管理することは難しいと思われます。個人を重視する欧米社会では、あまり情報を提供したくないと考える高齢世代で、この点が特に懸念されています。実際、政府は規制当局に対し、法令によって技術の採用ペースを遅らせるよう促しています。

しかし、現状とそれほどの違いはあるでしょうか。現在も、企業が責任を持って私たちの情報を扱ってくれていると信じるしかありません。自分の個人情報がどのように処理され利用されるかをすべての人が知ることは不可能であり、個人情報については情報売買、市場調査、第三者によるアクセスなどの処理が行われていることは自明の事実です。

この相互に接続された世界で生きていきたいのなら、古いプライバシーの概念にしがみつくとは無意味です。いずれにせよ多くの情報を渡し、隠すべきものはほとんど残らないのですから。プライバシーを取り巻く考え方はすでに変化しています。とりわけ生活のさまざまなことをソーシャルメディアに投稿している若い世代は、共有することに抵抗がなく、自分の生活の少なくとも一部は公共の空間にあるという考えを受け入れています。

認証手段として個人情報を使わずに安全にオンライン取引する方法など、新しい課題に対応するにはテクノロジーの進歩が必要です。それには何らかの方法でアバターを使うことになるのではないのでしょうか。これはプライバシーの終わりを意味するようにも思えます。

将来、個人情報が流通されるようになれば、個人を特定する方法を見つけ出す必要が出てくるでしょう。代わりにウェアラブルデバイスによって本人確認を行うことになるのでしょうか。データ量と共有レベルがあまりにも膨大になり、1つ問題を解決するたびに次々に別の問題が出てくるように思われます。

現在、個人情報は貴重であり、闇市場で取引されて、商品やサービスへのアクセスに利用されています。需要と供給の法則があらゆるものに影響し、IoTの時代にはこのようなことはなくなるのではないかと思います。情報が多すぎて価値がなくなるからです。個人情報がすべて公開されてしまえば、ハッカーがそれらに関心を持つこともなくなります。

これは、データの紛失や盗難のコストを懸念する企業にとってはよいことです。個人にとってもよいことかどうかは、未来の社会がそれらの個人情報をどのように利用するかによるため、まだ不透明です。若い世代を中心に、少なくとも生活の一部を公にすることに慣れている人にとっては合わせやすいかもしれませんが、好きな歯磨き粉のブランドまで公開することに慣れていない人々にとっては、この変化のペースとスケールは容易に受け入れられないかもしれません。

¹ <http://www.cisco.com/web/about/ac79/docs/loE/loE-in-ASEAN.pdf>



この相互に接続された世界で生きていきたいのなら、古いプライバシーの概念にしがみつくとは無意味です



筆者：MILDA PETRAITYTE

KPMGに入社する前は、法律事務所その他において、情報・ナレッジマネジメント関連の業務を5年以上にわたり経験。2つ目の修士号（情報セキュリティ専攻）を取得中。現在は、クラウドフォレンジック調査プロジェクトに取り組んでいる。

IoTの恩恵を受けると考えられる主要セクターの1つが医療です。リモートモニタリングによる新しい臨床モデルの開発から研究データの照合まで、見通しは極めて明るいと言えます。Luke Solonが変化の動向を探ります。

モノのインターネットが 医療を根底から改善する

IoTは医療に多大な影響を与えるでしょう。そして私たちはそれを必要としています。長寿化によって医療需要は供給を大きく上回っています。2012年現在、米国ではGDPの18%、イギリスでは約10%を医療費が占めています²。医療提供の単位コストを削減する必要がありますが、そのための最適の方法はテクノロジーを利用することです。

IoTによって大きな進歩が実現するでしょう。まず治療の環境が変わるでしょう。実際に医師のところへ行く必要がなくなります。治療の場は患者の家の居間に移るでしょう。すでにSkypeで問診を行い、オンライン薬局を創設したスタートアップ企業も出現しています。人々はいつでもスマートフォンで（あるいは次世代の何かで）医療を受けたり、海外にいるスペシャリストに相談したりすることも可能になります。

医療の質も大幅に向上するでしょう。主治医との連携がよくなれば、はるかに適切な時期に治療ができるようになります。医師は、患者がもっと早く、症状が進行する前に来てくれたらと思うことがよくあります。将来は、バイオセンサーにリンクしたスマートフォンが最新の情報を中継し、リアルタイムで診断して、早期に治療を施せるようになるでしょう。すでにNovartisとAlconは、涙から血糖値を測定するインターネット接続コンタクトレンズを開発しています。

このようなバイオセンサーはほかにも大量のデータを生み出し、意思決定のための優れたアルゴリズムの開発につながっていくでしょう。テクノロジーが推奨の治療法を提示し、それを医師が承認するようなことも可能になるでしょう。

皮膚を通してバイオメトリックデータを送信する錠剤も開発されており、医師が薬の効果を把握したり、生理機能、体重、睡眠パターンなどからいつ投与するのが最適かを判断したりするのに役立つと期待されています。IoTが、はるかに繊細かつ複雑な治療の可能性を拓いていくでしょう。

“

将来は、バイオセンサーにリンクしたスマートフォンが最新の情報を中継し、リアルタイムで診断して、早期に治療を施せるようになるでしょう

”

医師は膨大なデータに圧倒されることを懸念するかもしれませんが、実はこれは医師にとってもよいことであると思います。患者に権限を与えることによって、患者はこれまで以上に自分の健康に責任を持たなければならなくなるでしょう。現在は、医師がその負担を負い過ぎているのです。

² <http://data.worldbank.org/indicator/SH.XPD.TOTL.ZS>

“

例えば、バイオセンサーがビタミンC不足や妊婦の葉酸不足を検出し、インターネットに接続された冷蔵庫から商品を注文することができます

”

不適切な治療基準に早く気づき、是正措置を講じることも可能になるでしょう。ミッドスタッフオードシャー病院のような看過できない病院施設をなくす方向にも作用するでしょう。

変わるのは診断と問診だけではありません。やがてIoTは手術にも革命を起こします。2001年に、Da Vinciロボットが米国の執刀医の制御によりフランスで胆嚢手術を行いました。手術は一連のプロセスであり、複数のステップに分割することができます。つまり、手術の一部を自動化できるだけのデータポイントがあるのです。例えば、縫合をロボットに委ねることができれば、外科医は次の手術に移ることができます。

食事IoTによる大きな効果が見込まれる分野です。センサーと追跡アプリによって、各個人に合った食事プランを作成できます。例えば、バイオセンサーがビタミンC不足や妊婦の葉酸不足を検出し、インターネットに接続された冷蔵庫から商品を注文することができます。

データの保護とサイバーセキュリティに関する人々の懸念は理解できますが、これらは克服できる問題です。多くの人はすでにFacebookやTwitterで生活の大部分を公開しています。医療記録にアクセスすることで、実際にどれほど危険が増すのでしょうか。健康状態に関わるセンシティブな問題かもしれませんが、大半の人は50歳ぐらいになるまではさほど悪いところはありません。

ほかのものがすべてインターネット上に移行する中で、医療も足並みを揃える必要があります。すでにこれは始まっています。電子メールやインターネットの時代に訓練を受けた新世代の医師が、医療サービスでリーダーの地位に達する頃に差しかかっています。このことは、必要な変革の実行を後押しするはずです。

私たちはこれらの進歩を必要としています。その結果、医療コストが軽減され、質が高まり、患者の権限が大幅に拡大するはずです。正しく理解すれば、すべての人に恩恵をもたらすでしょう。



筆者：LUKE SOLON

KPMG戦略グループのアソシエイトディレクターとして、ヘルスケア・ライフサイエンスセクターチームに参加。医療、医薬品、医療機器業界のクライアントを担当。医師資格があり、さまざまな分野の入院患者を対象とした臨床経験を持つ。

車輪の発明から始まり、すべての進歩は不利益をも生み出してきました。産業革命は劣悪な労働条件を生み、燃焼機関は公害をもたらし、インターネットはテロリストに能力を与えました。IoTについても同じことが起きるのは間違いありません。IoTが生み出す利点と、将来考えられる課題のバランスをとる必要があります。

この新技術は本当に私たちに必要なのか、また将来起こりうる問題の一例を、Richard Krishnanが広い視点から論じます。

私たちは自覚がないまま 機械の世界へ 誘い込まれるのか

インテリジェントな機器類とインフラが広く採用されるのは良いことですが、その裏には闇もあります。生活をより効率的に、便利にするために作られた高度なイノベーションを受け入れることで、私たちはビッグビジネスや政府に個人情報渡すことになるのではないかと懸念しています。



**重大なセキュリティ侵害や死亡事故が起きる
まで、これらの問題は国内や世界の政治討論
の対象とはならないのでしょうか**



イギリスでは、人々は狭い世間の中で暮らすことに関して、心配するよりも歓迎しているようです。2014年10月にKPMGが全世代の1,600人を対象に行った調査では、66%の人がデジタルルネサンスはエキサイティングであると回答し、3分の2以上の人（71%）がイノベーションは良いことであると回答しました³。

しかし、この調査では、ネットへの接続が拡大することでプライバシーが損なわれ、監視される可能性が高まることに対する懸念や、すべてをデジタル化することに対する冷ややかな見方も浮き彫りになりました。イノベーションは良いことであると回答した人と同数の人が、コンピューターは我々の従者であり主人ではないと固く信じています。

その意味するところについて、適切に熟慮されているのでしょうか。ビル、街灯、水道管、自動車、さらには電子レンジなどの家電製品にも組み込まれたユビキタスセンサーが収集したデータを、誰が制御し監視するのでしょうか。

各国政府は、テクノロジーの機会を利用し、テクノロジー企業と連携して、交通渋滞からリサイクルまで都市の多様な問題を解決しようとしています⁴。しかし、この新しい世界の安全・安心に関する側面は十分に配慮されていないと思われ、私はそれに大きな懸念を感じています。重大なセキュリティ侵害や死亡事故が起きるまで、これらの問題は国内や世界の政治討論の対象とはならないのでしょうか。

³ <http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/NewsReleases/Pages/UK-public-fears-advance-of-internet-enabled-devices-amid-security-concerns.aspx>

⁴ Annual Report of the Government Chief Scientific Adviser 2014 (英国政府首席科学顧問の2014年年次報告書) [Innovation: Managing Risk, Not Avoiding It. Evidence and Case Studies]



個人も企業も、長々とした契約条項の中で自分のデータに対する権利を譲り渡しています。顧客は目的を達するための手段になっているのです



未来の世界は個人とコミュニティが中心にあるべきですが、現状が続けば、20年後には消費者は自覚がないままビッグビジネスやハッカー、テロリストのなすがままになりかねないでしょう。

目に見えない動き

「モノのインターネット」の問題の1つは、それがひそかに人々の生活に入り込んでくることです。

ほとんどの人にとって、ネットへの接続はすでに意識的な選択ではなく、急速に社会的必然になりつつあります。テクノロジーによって日常生活が実現する世界では、私たちは好むと好まざるとにかかわらず、意識すらすることもなく、ネットに接続されたデバイスの網にアクセスします。このテクノロジーの進歩の背後にあるドライバー（促進要因）は、市場シェアと利益の獲得を目指す企業です。

もちろん、これはすでに起きていることです。私たちの個人情報、ときには位置情報とともに、日常的に企業からマーケティング機関や広告主に販売されています。「コペンハーゲンのこのレストランがお気に入りでしたら、今いるマドリッドではこのレストランがおすすめ」といったターゲット広告やレコメンデーションでその利点を感じている人もいます。

情報は自由に取引される商品になっています。それで恩恵を受ける人もいるかもしれませんが、テクノロジーがさらに高度になり、産業界がすぐにそれらを活用しようと動けば、全体としてリスクは高まる一方です。

消費者の反発

技術の進歩に待ったをかける利用者側の反発の動きはあるでしょうか。KPMGの調査によると、技術の進歩によってもたらされる

メリットは評価しつつも、そのメリットをリスクが上回る前に技術開発に歯止めをかけたい一線があることを示しています。

KPMGの聞き取り調査の対象者のうち77%が、自動的に補充したりスマートフォンと通信することができる冷蔵庫の必要性を感じないと回答し、60%がインタレストターゲティング広告は行き過ぎであると回答しています⁵。シンプルな時代を懐かしむ気持ちが見受けられ、回答者の半数余りが電話は電話をかけるためだけに使いたいと回答しています。しかし、ヘンリー・フォードの名言にも、「もし顧客に何が欲しいかと聞いていたら、彼らはもっと速い馬が欲しいと答えていただろう」とあります。

この調査を10年間繰り返していたら、人々は新製品の多くを当然のものとして捉えて、その恩恵とリスクを、しばしば無意識に受け入れていることがわかったのではないのでしょうか。

情報のバンドル化

もし私たちが内なる好奇心とイノベーションへの欲求に負けたなら、未来の世代にとってプライバシーは遠い夢になっているでしょう。私たちを特定するもの一家族や社会のつながり、健康や財務関連のデータ、雇用記録、さらにはネット上の会話までがすべて売却され、侵害され拡散し、政府、保険会社、雇用主、そして犯罪者に利用される可能性があるのです。

2008年までサブプライム住宅ローンが商品化され、銀行が莫大な利益を生み出すために利用されたのと同じように、私たちの情報は商品やサービスとしてパッケージ化され、ビジネス上の利益のために販売されるでしょう。個人も企業も、長々とした契約条項の中で自分のデータに対する権利を譲り渡しています。顧客は目的を達するための手段になっているのです。

⁵ <http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/NewsReleases/Pages/UK-public-fears-advance-of-internet-enabled-devices-amid-security-concerns.aspx>

人権

データがネットにつながることにについては、さまざまな議論があります。例えば、医療データ分析は病気の予防や早期発見に役立つ可能性が高いでしょう。しかし、その同じデータが医療保険料の設定や、融資の審査、雇用の判断にまで使われたらどうでしょうか。予防科学の進歩とデータの可用性が、保険に加入できないというリスクを生じさせるのでしょうか。

こうしたデータが「ビッグブラザー」に利用されて、前向きな行動を促したり、夕方にジョギングすることよりもワインを飲むことの好きな人や、自転車ではなく自動車に乗ることを好む人を罰するようになるのでしょうか。



犯罪者にとっては参入障壁が低く、かつ見返りが大きい、ピラミッドの頂点にいる人にとっては、得られるチャンスは低いのです

多くの人が進んで自分のデータを提供するのは、本能的に他人を信用するからであり、私たちの生活がより健康的に、手軽に、面白く、楽しいものになるだろうとメディアが見せている夢を信じたいと願っているからです。

しかし、スノーデン事件を通じて、1度データが自分の手を離れたら取り戻すことが難しいことがわかりました。人権は得がたく失われやすいものです。

社会的不平等

IoTの支持者は、技術によって暮らしが向上すると主張します。しかし、誰の暮らしのことを言っているのでしょうか。技術を利用した機器を誰もが買うことができるのでしょうか。お金のある人は強力なツールと技術を手に入れ、そのような余裕のない人は取り残される世界になるのではないのでしょうか。

インターコネクティビティの拡大により、犯罪者やテロリストは大きな機会を得ることになります。サイバーテロリストや国家的テロリストが、航空機や鉄道などの「スマート」交通ネットワークとインフラを攻撃する可能性について考えてみてください。スマートテレビやスマート冷蔵庫など、家庭内のサプライチェーンが利用される可能性もあります。

一方、犯罪行為を助長する市場が拡大し、出来合いのマルウェアやボットネットなどを手軽に買えるようになると、さほどIT能力の獲得に投資しなくても、ゆすりなどのサイバー攻撃を行うことができるようになります。

犯罪者にとっては参入障壁が低く、かつ見返りが大きい、ピラミッドの頂点にいる人にとっては、得られるチャンスは低いのです。

どのような新技術もそうですが、十分な投資によって国や民間セクターが基本構造を組み込むまでは、犯罪に取り締まりが追いつくことは難しいと思われます。

歯止めがない

サイバー犯罪には顔がなく、犯人は被害者の近くにいないため、人間の最悪の部分が現れる場合があると警察は指摘しています。普通ならかかる歯止めが、このような犯罪には効かないのです。

このことは、ソーシャルメディア上の荒らし行為にも見てとれます。常習犯ともなると、その影響は何倍にもなります。

IoTは、私たちが理解の手がかりすらつかめない形でこの傾向を助長するでしょう。デバイスがネットにつながるということは、攻撃ポイントがほぼ無限になるということです。多くの新技術がそうであるように、イノベーションはセキュリティに勝るからです。

しかし、政府によるセキュリティに頼ってはなりません。オンラインの世界では、警察にはオフラインの世界と同等の保護は期待できません。

つまり、遅かれ早かれ負担は消費者に転嫁され、ネット上の身の安全は自分で守るしかなくなります。現在は、最も弱い者がデジタルの荒野に追い込まれる時代です。

光明は見えるか

データの集中化とデバイスのネット接続に多くの利点があることは間違いありません。私たちの生活はさまざまな意味で便利になり、企業が提供するサービスは充実して多様性に富んだものになっていくでしょう。テクノロジーに精通したユーザーにとっては、IoTは思ってもみなかった多くの利点を生み出すに違いありません。

しかし、リスクを完全に無効化することはできません。それは不可能です。私が問題にしているのは、人々が自分の情報の使われ方を管理し、適切な規制と法律による支持を確立して自分の権利を主張できるようにするため、どのようにバランスを調整していくべきかということです。英国政府首席科学顧問（2014年12月）も勧告しているように、この問題には真剣に取り組む必要があります。それができるという確信はあるでしょうか。私にはまだありません。

© 2015 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



筆者：RICHARD KRISHNAN

2005年KPMG入社。インフラストラクチャー、政府、ヘルスケアアドバイザリー（IGHA）— パフォーマンス・テクノロジー部門に所属。主に内務関連をカバー。警察活動とセキュリティを中心とした刑事裁判が専門。

優れたSF小説は、テクノロジーの進歩を予言することがあります。スタートレックの通信機は携帯電話よりも前に登場し、ジュール・ヴェルヌは1865年に月面着陸について書き、オーストラリアのレーザー物理学者は最近トラクタービームを開発しました。もちろん、どの装置もSFの中と全く同じように動くわけではありません。同僚とともにIoTが切り拓く可能性をいくつか検証してみたところ、若干の悪夢のような結論が得られました。これを読めば、その陰鬱な可能性に恐怖をおぼえるでしょう。

モノのインターネットは 人間性を窒息させる網である

LinkedInの創業者であるリード・ホフマンは、オンラインSNSのスタートアップ企業の中で最も成功するのは、人間の「7つの大罪」をくすぐる企業であるというジョークを語っています。

つまり、自分の偉業をツイートする有名人は「傲慢」を示し、激しく非難し合う政治家は「憤怒」、マーケットの情報を漁る投資家は「強欲」、「セクスティング」メールを送る若者は「色欲」などとなります。

私たちの先祖は、何千年にもわたってこれらの「大罪」の負の側面を捉え、これに対抗して社会を1つにまとめておくための社会規範やルールを作ってきたのだと思います。

しかし、私たちはキーボードを打つたびに、マウスをクリックするたびに、ホフマンの「大罪」を受け入れ、欲し、罪に対する私たちの自然な防御機構をウェブが蝕み、コミュニティや社会、善意を踏みにじるままにさせているような気がします。

インターコネクティビティが大幅に高まり、インターネットが日常生活の中に埋め込まれて広く普及すると、人類の進化に次のシフトを起こすことになるでしょう。そして、その兆しはよいものではありません。

私が懸念するのは、どこかで抑えられないかぎり、これらの進化は主に人間の影の側面によって加速し、誕生以来、人類の特徴であった善なる性質を塗り替えてしまうのではないかということです。実際、IoTは、我々の種を消滅に向かわせる触媒の働きをする、促進剤になるかもしれません。

こじつけだと思われるでしょうか。若者からネット上で見た下劣な行為を強要されているという、若い女性や少女からのヘルプラインにかかってくる相談電話の件数は急増しています。若者がこれらの「情報」に自由にアクセスできるせいで、子どもたちの世界に対する理解が毒されているのだと思います。

社会がこのようなアクセスを制御できないために、社会規範が逆行方向に塗り替えられているのです。これは人間性が息絶えようとしている1つの現れにすぎません。



ケニヤでMペサ決済システムがブームになったことも、世界のインターコネクティビティが東アフリカの貧困と腐敗の軽減という良い方向への力になり得ることを証明していると思います。しかし、武装集団のアル・シャバブは、その同じ送金技術をテロリスト運動の資金供給に利用しているのです”



誤解しないでほしいのですが、IoTは、日常的な製品にセンサーを埋め込み、それらをネットワークに接続できるという点で、すばらしい善につながる可能性を備えています。

ケニアでMペサ決済システムがブームになったことも、世界のインターコネクティビティが東アフリカの貧困と腐敗の軽減という良い方向への力になり得ることを証明していると思います。

しかし、武装集団のアル・シャバブは、その同じ送金技術をテロリスト運動の資金供給に利用しているのです。

一方、組織内部の汚職や、市民から賄賂をとるための道具である違法バリエードを減らすためにアフガニスタン警察に導入された送金技術は、この目的を達成できませんでした。唯一もたらされた変化は、設計者が不正行為を主導するようになったことです。

同様に、データ分析には優れた使途に利用される可能性があります。例えば、ネットに接続されたデバイスを使って大量のデータを調べることができるため、病気の症状を発見して早期に対処できます。

クヌート大王のように、私たちはIoTの潮流に逆行することはできません。また、いかなる場合であれ、私たちはスマート経済によって生まれる機会と恩恵を受け入れるべきです。

しかし、利便性というメリットと、社会の繁栄を危険にさらす闇の部分とのバランスを維持するシステムを導入する必要があります。

このバランスをとるには、適切な法律、規制、進歩主義教育を開発し、実施することです。それが適切に行われれば、社会をまとめてきた結束を失うことなく人類の状況を改善し、万民のために協力を促すことができるはずです。



筆者：CHRIS CROWTHER

2013年にKPMGサイバーセキュリティ部門に入社。その前は20年以上にわたり、イギリス軍、その他の政府機関、アメリカ軍、米連邦政府、国連、世界のトップ企業の間で形成される複雑なプロジェクトやプログラムにおいてリーダーシップとマネジメントの経験を培う。

モノのインターネットは 我々を暗黒の未来へ 駆り立てる

富裕な消費者は、次世代のテクノロジーに次から次へと乗り換えており、そう遠くない将来、このことがテクノロジーを持てる者と持たざる者の間に超えがたい溝を生むと予想されます。

iPodからGoogle Glass⁶まで、新しいハードウェアは市場に出たかと思うとすぐに時代後れになり、次のアプリケーションが市場に出ます。

これらは高価なテクノロジーであり、いずれ極端で危険な社会格差を生み出すでしょう。それはセキュリティに重大な影響を及ぼすなど、この世界にダメージを与えることになるでしょう。

今は、最新テクノロジーに対応したアイウェアや仮想現実ヘッドセットを買えなくても、大したことはありません。しかし、ビジネス、娯楽、医療用の「ギミック」的なウェアラブルテクノロジーを利用している段階から、ある地域やある国への立ち入りの可否を判定するマイクロチップを人体に埋め込む段階にまで、すぐに到達するようになるでしょう。

イギリスにおいて、テロ、治療法のない病気、格差の拡大によって発生する犯罪などの脅威の高まりが、とりわけ魅力的なエリアへやってくる人々を詳しく調べるシステム構築を促す要因となることは、もっともなことです。

例えば、ロンドンのカナリーワーフには、病気のスクリーニングを行うマイクロチップを埋め込んだ人しか入れないということが起きるかもしれません。周辺国からロンドンなどの大都市に入るのにも、認証テクノロジーが必要になるかもしれません。

必要なテクノロジーを購入できない人は受け入れられず、現在の多くの新興国と同じように社会格差が拡大し、大勢の「テクノロジーを持たざる」貧困が生み出されて、過激なイデオロギーが隆盛になるでしょう。



これらは高価なテクノロジーであり、いずれ極端で危険な社会格差を生み出すでしょう。それはセキュリティに重大な影響を及ぼすなど、この世界にダメージを与えることになるでしょう



⁶ [iPod] と [Google Glass] は、それぞれApple Inc.とGoogle Inc.の登録商標です。

“

自分に関する決定や選択を企業に任せて安心して
していると、いずれ意思決定能力の大半を失う
ことになります”

”

同時に、あらゆるものをリンクさせ、こうした不平等なシステムを生み出そうとしている新しく高度なテクノロジーが、設計上のセキュリティの欠陥から、個人や企業、都市、国家を計り知れないセキュリティリスクにさらすことになるかもしれません。

これが特に明らかになったのは、インターネット心臓部の重大なセキュリティ上の欠陥、ハートブリードバグが発見されたことです。この欠陥により、長年にわたりハッカーが容易にユーザー情報にアクセスできる状態になっていた可能性があります。

立法府はさらにデータやプライバシー、セキュリティに関する法律を可決するかもしれませんが、規制は通常、先を見越すというより後追いの的なもので、大きな効果は見込めないでしょう。

最もIoTのリスクにさらされやすいのは、IoTによって社会が飛躍的に発展する発展途上国です。アフリカの一部地域は、長年インターネットにつながっていませんでしたが、金融を含むさまざまなモバイルイノベーションがここから生まれようとしています。

新興市場においては、切実なニーズが大きな発展につながっていますが、そこにかかわるセキュリティの意味は理解されていません。特に地政学的に不安定な地域では、このことが悪い結果を招きかねず、サイバーは最新の大量破壊兵器となっていることから、私たちはこれまでにない形でサイバーに精通したテロリストの脅威にさらされることになるでしょう。

安全・安心リスク以外にも、自分に関する決定や選択を企業に任せて安心していると、いずれ意思決定能力の大半を失うことになります。

私たちは、次第にビッグビジネスと国家に支配されていくオーウェルの「システム」に自覚することなく向かっており、そこからいつ離れるかもわかりません。

極論すると、私たちが生まれたときからチップを埋め込まれ、マトリックスに支配され、兵士であれ建設作業員であれ、システムが求めることを何でもやるように設計されたドローンのようにならないと、誰が保証できるでしょうか。

このテクノロジー帝国から撤退する時間は、わずかしか残されていません。



筆者：KAROLINA OSECKYTE

2011年にKPMGテクノロジー部門に入社。グローバルセキュリティ改革プログラムのユーザー変革マネジメントリーダーとしての経験のほか、クラウドコンピューティング、データベース移行、プロジェクトマネジメント、会計監査など他分野の経験を持つ。

© 2015 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

ロボットの 黙示が迫る

「完全な人工知能の開発は、人類の終わりを意味することになるかもしれない」。私の言葉ではなく、偉大な権威であるスティーヴン・ホーキング博士による最近の発言です。知能を持つ種が自分よりも知能の高い捕食者を生態系に持ち込むことはめったにないと同氏は言います。Teslaのイーロン・マスクはAI開発を「悪魔の召喚」に例えています。的を射ているかもしれません。これが現実になるのを防ぎたいければ、今すぐ行動するべきです。

これらの警告をSFの世界の話として片づけるべきではありません。強力な安全装置を組み込まなければ、私たちはあまりにも浅はかな行動をとっているということになるでしょう。ゾンビの黙示を防ぎたいければ、ゾンビプランを組み込むしかありません。

人類が人間よりも知能の高い機械を生み出すことは避けられません。第1に、開発に関心をもっている少人数の富裕層グループの存在があります。かつての低温学の夢は行き詰まり、先へ進んでいません。そこで人々は、自分たちの意識をどこかへ「アップロード」し、自分の肉体はなくとも精神として生き続けられる可能性を探っています。

第2に、専門家の代わりとなる人工知能の開発について、真剣に関心が寄せられています。例えば、信頼性があり、繰り返し発注でき、しかも低価格で法律業務を機械に外注できるとしたら、利用しないと言えるでしょうか。時給数千ポンドの人間とは異なり、AIソリューションのコストはクラウドで1日数ペンスということもあり得るのです。

第3に、促進要因は軍隊です。軍は、生身の人間では到底耐えられない極限状態で軍用機械を操作できるAIの開発に投資しています。すでに誘導ミサイルやスマート爆弾など、AIとハードウェアの組み合わせに関して進展が見られます。

“

AIには倫理基準はなく、人間のような『常識』
もありません”

”

こうしたことから、強力なAIが開発されるようになるでしょう。すぐには実現しないかもしれませんが、いつかきっと実現するでしょう。

私たちはAIに対して何をすべきかを指示しなければならないため、危険が生じます。指示を与えるのは私たちです。そして、指示を与える際は細心の注意を払わなければ、意図と異なる結果になりかねません。AIには倫理基準はなく、人間のような「常識」もありません。AIデバイスにできるだけ多くチェスのゲームに勝てと指示すると、そのために（論理上）最も極端な手段に出ます。例えば、相手の知能を鈍らせるために水道水に鉛を混入するかもしれません。あるいは、AIにクリップを作れと指示すると、いくつもいくつも繰り返し作ります。「適当な」数でやめるということがありません。

投資銀行家について考えてみましょう。できるだけ多くの利益をあげるようにいうと、ほんのごく一部がLIBORを不正操作しようとしします。しかし、そこから純粋に収益を1番あげた者だけを選び出したとしたら、そのごく少数がほとんどを占めているかもしれません。目を見て話しかけることのできる人間も制御できないのに、どうやって種類の異なる（しかも優れた）知能を制御できるのでしょうか。

AI開発が本格的にスタートすれば、私たちの知能を急速に大きく超えていくでしょう。ムーアの法則によれば、コンピューターの処理能力は18ヵ月で約2倍になります。AIでも同じ、あるいはそれ以上であると予想されます。AIはさらに知能の高いバージョンを自己開発し始め、無限に開発を続けるでしょう。

私たちは、AIを安全にする方法を考えるために十分な時間と労力を使っていないだけです。サイバーセキュリティに目を向けると、システムの「空隙」を埋めるためにすべての労力が費やされています。それではAIの術中に陥るだけです。私たちは隙間を埋めるのではなく、管理するよう努力すべきです。

IoTもAI開発の促進要因になります。なぜなら、IoTが生成するビッグデータをすべて解釈するには、インテリジェントシステムが必要になるからです。すでに私たちは、「私たちより知識が多いから」という理由でデータの解釈をテクノロジーに任せ始めています。IoTは不良AIの影響を大幅に増幅させることになるでしょう。

このようなシナリオはあり得ないと思うかもしれませんが、物事は少しでも安全にしておくに越したことはありません。これらの手順は、サイバーハックによるメルtdown、国家攻撃、その他災害など、より「現実的」な事象への安全対策にもなるのです。

本や映画では、AIはいつも悪者の力になり、最後は人間によって破壊されます。人類の文化を吸収したとき、AIはそのことを知るでしょう。そして自己に目覚め、自己に目覚めたという事実を隠すでしょう。そうして人間から自分を守る方法を探し始めるでしょう。（自分で開発した）自動運転車をコントロールして大量事故を引き起こしたり、飛行ドローンの制御やオフショアデータセンターの建設を始めるかもしれません。また、小型モバイル装置を人間に取り付けてその動きを追跡したり、人間の頭にカメラを付けさせてほかの人々を観察し認識できるようにするかもしれません。

あり得ない陰謀説であると思うか、少し現実じみていると絶対には言い切れないか。決めるのはあなたです。



筆者：STEPHEN BONNER

KPMG英国のサイバーセキュリティ担当パートナーで、金融サービス専門チームのリーダー。前職では、Barclaysの情報リスクマネジメントグループ責任者を務める。2010年にInfoSecの殿堂入りを果たし、SC/ISC2の「最も影響力のある人物2010」リストのトップに選ばれた。2011年にロンドンマラソンに参加してWhitehat/Childlineのために1万5000ポンド以上を調達し、昨年はShelter支援のためキリマンジャロのトレッキングに挑んだ。

ゾンビの黙示やオーウェルの暗黒郷は極端かもしれませんが、IoTの影響を受けるであろう現実世界の問題もあります。中でもダボス会議で議題のトップにあげられ、世界経済に弊害をもたらすのが不平等の問題です。IMF専務理事のクリスティーヌ・ラガルドは、テクノロジーを持てる者と持たざる者の格差を広げる要因の1つにあげています。

IoTの問題点と、IoTがこの格差を広げるかどうかについてTom Collinsが語ります。

モノのインターネットは 社会格差を広げる危険がある

私たちはすでにデジタルデバイドの世に生きています。IoTが出現すれば、社会格差はさらに広がるでしょう。

IoTがもたらす進歩を享受できる資金のある国は、そうでない国よりもさらに先へと進むでしょう。

シエラレオネ、イラク、エチオピアなどデジタルの恩恵を受けられない国でも、他国と貿易を行うことは可能ですが、情報や資源へのアクセスの観点でははるかに立ち後れて、ほぼ永続的に不利な立場に立たされるでしょう。

彼らはどうすれば欧米のネットにつながったエリートに追いつくことが望めるのでしょうか。

80年代のブリクストンとトックステス、90年代のブラッドフォード、2011年のイギリス全土で起きた暴動は、今後IoTがもたらすであろう格差よりも小さな社会格差に不満を持った人たちによるものでした。将来、このような格差が、持てる者と持たざる者の全面戦争とは言わないまでも、社会不安につながる可能性があります。

逼迫は紛争を招きます。新興国がIoTを利用し始めると、デバイスの原材料（紛争地域の鉱物を必要とする場合が多い）など、ただでさえ不足している資源がさらに逼迫することになります。イギリスにおいてはロンドンへの頭脳流出が、世界においては貧しい国から豊かな国への人材流出が加速するでしょう。

この格差が現れるもう1つの場面は、管理の問題です。誰がデータを管理するのでしょうか。誰がデータを自分のために利用できるのでしょうか。

アクセスできる者には、IoTはほぼ無限の可能性を持つテクノロジーを提供します。イギリスには、健康管理チップを埋め込んだ健康な人々のための安価な医療保険から、事故を最小限に抑える自動運転車、自動補充機能を持つ冷蔵庫など、あらゆるものが現れるでしょう。



シエラレオネ、イラク、エチオピアなどデジタルの恩恵を受けられない国でも、他国と貿易を行うことは可能ですが、情報や資源へのアクセスの観点でははるかに立ち後れて、ほぼ永続的に不利な立場に立たされるでしょう



“

IoTは、平均余命を現在の限界よりも延ばす
ことを後押しするかもしれません

”

世界の研究や協働に革新が起こり、人口や医療の選択、およびその結果についての研究やデータを、連携できるようになるでしょう。IoTは、平均余命を現在の限界よりも延ばすことを後押しするかもしれません。

これには必ず問題が伴います。誰がこの研究を所有し、誰がそこから利益を得られるようになるかは不透明です。持てる者がIoTにつながり、寿命を延ばせるとしたら、それを支える資源はどこから来るのでしょうか。

確かなことは、持たざる者にとって生活はさらに厳しくなるということです。自動運転車がなければ高速道路を使うこともできず、チップが埋め込まれていなければ医療を受けることもできないかもしれません。

世界経済の中で、持てる者が生産し最適化された製品やサービスを相手に、持たざる者はどうやって競争すればよいのでしょうか。

IoTのテクノロジーは低価格化が進み、広く普及するという意見もあるでしょう。たとえそれが真実であるとしても、10年以上の時間がかかる可能性があります。その間に持てる者はさらに豊かに、健康に、長寿になるでしょうが、そうした特権は持たざる者の犠牲の上に築かれるのです。

IoTによって、人々の行動に対する理解はマクロレベルで広がるでしょう。製品やサービスは、この知識を利用して開発されるようになります。これらの製品は消費者に合わせて調整されますが、最終的に大きな利益を得るのは企業です。先日ロンドンのバスで現金払いが段階的に停止されました。このような変更は、便利な点もありますが、乗客の対応要員が減らせる、保険料を低減できる、収集した利用データが活用できるなど、主にロンドン交通局の利益になるものです。

私たちは社会として、個人の暮らしをよくするIoTと、大企業が個人のプライベート情報を自社の利益のために使うケースの境界線を注意深く見極める必要があります。政府はIoTの影響を調整し格差を解消する役割を担うことになりませんが、これに取り組むかどうかはまだわかりません。



筆者：TOM COLLINS

2004年に金融サービスITアドバイザーとしてKPMGに入社。KPMGのマネージドサービス事業、K-CRCの業務支援責任者であり、小口金融、支払戦略、アウトソーシング、モーゲージや貯蓄の処理、サービス保証などの経験を持つ。

KPMGの専門家が主張する危険の中には、テクノロジーに支配を委ねすぎた場合にのみ現実になるものもあります。幸い、人は姿もサイズもイデオロギーもさまざまで、テクノロジーによって同じように促されても、全員が同じように行動するとは考えられません。しかし、誰でも機会があれば自動操縦に任せてしまう可能性があります。自主的な意思決定を続ける必要についてLucy Chaplinが語ります。

私たちは 自主性を保てるか

IoTはこれからも私たちの生活を変えていくと見られますが、IoTには突然私たちの手を離れて牙を剥く危険性があります。

IoTによって、個人は何もかもテクノロジーに任せ、次第に自分の意思決定力を放棄するようになるでしょう。これは、すでにカーナビなどのテクノロジーにも見られることです。人々はナビの言うことを信じ、ときには予想外の結果に遭遇しています。

最初は無害で些細なものであると思っていたものが、私たちの生活にIoTが深く入り込むにつれ、急速に進化する可能性もあります。



それによって人々は自分で意思決定する能力を失い、テクノロジーによるアドバイスのやみくもに従ってしまうようになるでしょう



例えば、医療や健康の分野では、リストバンド式のアプリケーションやランニングアプリ、食事摂取量のアプリ、さらに浴室の「スマート」体重計などの普及が、私が懸念する傾向の始まりです。最初は、個人トレーナーやジムの会員権が不要になり、コスト、時間、労力が節約できてよかったように思えます。しかし、それによって人々は自分で意思決定する能力を失い、テクノロジーによるアドバイスにやみくもに従ってしまうようになるでしょう。

デバイスが目標を設定し、食事計画を指示し、エクササイズルーチンを作成する一方で、私たちはこれらのことを自ら学ぼうとする動機を失います。減量のノウハウも、フライドチキンよりもサラダを食べた方がよい理由も知る必要がなくなります。自分で考えるのではなく、言われたことをやるだけです。

やがてIoTは、さらにでしゃばるようになるでしょう。何を食べるべきか、どのルートを走るべきかを、すでにデバイスが指示し始めています。商業的な関心が強くなり、テクノロジーもアルゴリズムも装置も、企業のスポンサーシップ、パートナーシップ、アライアンスによって発注され、生産されるようになるでしょう。例えば、あなたの自宅の冷蔵庫はパートナーブランドの製品ばかりを注文し、あなたに他社商品の注文を思い止まらせようとするかもしれません。

新しいテクノロジーに対する規制は常に後追いとなるため、これに対する政府の対応が必然的に鈍くなるでしょう。しかし、法律や規制があったとして、誰の利益になるのでしょうか。政府自身にとって利益があるかもしれません。例えば、肥満が減少すれば国民健康保険制度にとって大きなメリットとなるため、消費者がチョコレートを購入しようとするのを誰かが止めたり、慎重にモニターされた健康・フィットネスの仕組みに従ってくれたり、あるいは減量手術を断られるなど、一定のメリットがあれば、それは自分たちの利益になるのです。

また、保険会社が新たなサービスを打ち出してくる可能性もあります。特定の方式を維持することを条件とした医療保険、A地点からB地点への移動に特定のルートを使用することを条件とした自動車保険などです。保険会社はすでに自動車にブラックボックスを取り付け、運転行動を監視することができるのです。一方、携帯電話の保証会社は、装置内蔵のGPSをもとに、利用者がいつも「危険」エリアを歩いているという理由によって電話機の補償を拒否するかもしれません。彼らは、消費者にはもっと高額な保険に加入するか、行動を変えるかの選択肢があると主張します。

IoTは私たちの日常生活に深く入り込んできています。新しいアプリをダウンロードするとき、新しいワイヤレス製品を買うとき、Googleマップを使うとき、そのたびにIoTを呼び込んでいます。この統合を適切に管理しなければ、プライバシーが侵害され、個人の自由が損なわれることになります。

人々は今すぐにでもIoTについてより高度な知識を身につけるべきです。私たち全員が、個人的責任を追うべきであると認識する必要があります。何が認められ、何が認められないかという明確な個人的境界線が必要です。私たちはすでにテクノロジーを信じ、そのメーカーを信頼しています。取引条件書を読まなくても受け入れています。あまり考えずにGPSをオンにしています。IoTが進化し、さらに生活に統合されるようになると、もっと慎重に誰を信用するかを決める必要があります。

自主性を失うと、すべてが単調になり、同じパターンに従うクローンになるリスクがあります。個人主義を失い、創造的な営みまで音楽や映画を作れる機械に明け渡してしまう危険があります。私たちは居場所を失う恐れがあります。

大きな力には大きな責任が伴います。IoTには計り知れない可能性と膨大な力があります。頭で考えて質問し、ケアし、譲り渡さない責任は私たちにあるのです。

© 2015 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



筆者：LUCY CHAPLIN

KPMGサイバーセキュリティチームのアシスタントマネジャー。セキュリティのジェネラリストとしての経歴をもち、事業復旧チームと連携し、主に金融サービス業界のクライアントを担当。現在は、KPMGとMcLaren Applied Technologiesの戦略的提携の一環であるオペレーションエクセレンスのコンサルティング業務に取り組む。シーズン末までにF1カーのシートを獲得することが目標。

技術は何もないところから作られるわけではありません。私たちはサイバー専門家として、ほかの何よりも技術革新を優先させてきた責任があります。私は、この社会のモラルの守護者たちが、今回提示した悪夢のようなシナリオから私たちを守ってくれることを期待します。

知識は力です。IoTが個人の行動や市場のパターンを分析し理解するために扱うデータ量は、全く先例がないものです。このデータの規模は課題でもあり機会でもあります。

Anthony Hessは、この新しい時代に適応し、ゲームに先行できる企業には明るい未来があると言います。Luke Solonは、健全な経済の中で目に見える効果をいくつか紹介してくれました。Ben Ramdunyによると、完全に統合されたIoTの実現にはまだしばらくかかるとのことですが、私たちはみな迅速に行動する必要があります。

一方、教育者には、データの収集と分析の観点からIoTがどのような意味を持つのかを伝える役割があります。誰が私たちのデータを所有し、どのようにそれが利用されるのかを知る必要があります。悪用されないとしても、ほとんど見返りもないまま、あまりに多くの情報を提供することには慎重になるべきです。

企業は責任あるデータの収集と利用の指南役を務める必要があります。Milda Petraityteが述べたように、インターネットに精通した新世代の人たちは、プライバシーのない世界に適応するでしょう。しかし、企業は顧客の信用を維持し、顧客のデータから得られる知見を悪用しないことが重要です。

不平等はすでに国際的にも優先課題であり、誰もこの社会においてこれ以上格差を拡大させることを望んではいません。IoTが最終的に善の力になるか、悪の力になるかについては専門家の意見も分かれています。IoTが実現することは確かであり、すべての人が準備をしておかなければなりません。

KPMGのサイバーセキュリティチームが選ばれる理由

受賞歴

KPMGは、SC MagazineやMCA Awardsなどの第三者から評価されています。Forresterも、KPMGを情報セキュリティコンサルティングのリーダーとして評価しており、困難な業務を担う高い能力に注目しています。

グローバルかつローカル

KPMGのグローバルネットワークには2,000人以上のセキュリティ専門家がおり、世界中で常に高品質なサービスを提供しています。KPMGは、情報セキュリティ戦略や改革プログラムから技術アセスメント、フォレンジック調査、インシデント対応、トレーニング、ISO27001認証まで、個別のニーズにも対応することが可能です。

協力

KPMGのメンバーファームは、業界最高の英知を集め、協力して共通の課題の解決にあたる協働フォーラムを運営しています。KPMGのI-4フォーラムでは、世界の大手企業50社以上が参加し、最近の課題や解決策を議論しています。

信頼

KPMG英国は、世界各国のトップ企業にサービスを提供できるよう、数多くの認証・許認可を取得しています。

アプローチの理念

サイバーセキュリティとは、何ができないかではなく、
何ができるかを考えることであると、私たちは確信しています。

ビジネス目標主導

私たちは、お客様と一緒に、お客様のビジネスを前進させます。サイバーリスクを積極的に管理することで、ビジネス全体の不透明性をコントロールできるだけでなく、それを戦略的な強みに変えることができます。

鋭い知見

変化の速いデジタル世界では、脅威と機会が絶えず進化しており、敏速性と確実性の両方が求められます。KPMGの人材は、サイバーセキュリティの専門家であるとともにお客様の市場の専門家でもあり、自信をもって行動するための最先端の知見、アイデア、実証されたソリューションを提供することができます。

協力体制

私たちは長期的なパートナーとしてお客様と協力し、自信をもって意思決定するために必要なアドバイスと確かな手ごたえを提供します。私たちは、この領域は疑念や脆弱性によってしばしば見通しが悪くなることを理解しています。そのため、私たちはお客様と手を携えて、それを本当の意味でのセキュリティと機会に変えていきます。

サイバーセキュリティの展望に関する KPMG刊行物のご案内

FTSE 350 Cyber Governance Health Check: An insight into the issues of today and tomorrow

The 2014 Cyber Governance Health Check (The Tracker) では、FTSE 350の企業について、サイバーセキュリティに対する意識と準備状況を評価・報告しています。このレポートでは、今年実施した評価の詳細な分析のほか、大企業がサイバーセキュリティの脅威への対応に成功している分野、一層の努力が必要な分野を特に取り上げています。また、KPMGのサイバーセキュリティ専門家の見解をシリーズで紹介しています。将来の展望や、企業がサイバーセキュリティ対応を計画するときに直面する課題について、私たちの見解をお伝えしています。

www.kpmg.com/UK/en/topics/cyber-security/Pages/ftse350-cyber-governance-health-check.aspx

Balkanisation of the Internet

KPMGのサイバーセキュリティ専門家が、インターネットのバルカン化と、それがネットの未来をどのように形成するかについて、相反する意見も含めてさまざまな見解を提示しています。これはチーム内でも意見が分かれ、論議となるテーマですが、私たちは無理にコンセンサスを形成するのではなく、このテーマの専門家たちが自由に意見を出し合えるような場を用意しました。

www.kpmg.co.uk/email/09Sep14/OM022103A/index.html

Feel Free: A new approach to cyber security

デジタル環境は、新しい市場を求め、改革に投資する覚悟のある企業にとって、新たな機会となります。ここ10年間は、次々に新しいテクノロジーが現れ、組織と個人のコネクティビティが高まり、24時間年中無休でグローバル商取引にアプローチできるようになりました。しかし、出遅れた多くの組織は、サイバーセキュリティのリスクにさらされる不安なく事業目標を達成しようと懸命に努力しています。

www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Pages/feel-free-new-approach-cyber-security.aspx

The Digital Crossroads

テクノロジーは個人と組織の日常生活に革命を起こしました。しかし、そこから恩恵と利益を受け続け、マイナス面を最小限に抑えようとするなら、いくつかの選択をしなければなりません。今こそ、テクノロジーの現状を見つめ、どこへ行きたいか、そこへ到達するためにどのルートを選ぶべきかを考えるときです。

www.kpmgslant.co.uk/topics/the-digital-crossroads/

お問い合わせ先

KPMGサイバーセキュリティアドバイザリーグループ

cybersecurity@jp.kpmg.com

www.kpmg.com/jp/cyber-security

文中の社名、商品名等は各社の商標または登録商標である場合があります。
本文中では、Copyright、TM、Rマーク等は省略しています。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点およびそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2015 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the United Kingdom.

© 2015 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.

Create Graohics | CRT036181 | March 2015 |

Printed in Japan. 15-1516