ＢＳＫ第２９－３号

# ＩｏＴのリスク管理

「Managing Risk for the Internet of Things」

Center for Strategic & International Studies (CSIS)
（戦略国際問題研究所）

平成２９年８月

公益財団法人　防衛基盤整備協会

# はしがき

本小冊子は、２０１６年２月に米国戦略国際問題研究所（Center for Strategic & International Studies：以下、CSIS）が、ウェブ上で公表している資料「Managing Risk for the Internet of Things」を翻訳したものです。「ＩｏＴのリスク管理」と題して翻訳しましたが、ＩｏＴのリスク管理に関する政策の策定を導く一つの方法として、リスクをどのように測定するかを検討したものです。

ＩｏＴは、１９９９年にケビン・アシュトンによって最初に使用された言葉ですが、ＩｏＴがビジネスの分野でも使われるようになったのは、スマートフォンが普及した２０１０年です。この頃、ＩＴ企業が未来のスタイルとして、ＩｏＴを活用するようになりました。ＩｏＴデバイスの数が増え続けるにつけ、企業、消費者等は、利便性と生産性の向上というメリットを享受しています。しかし、ＩｏＴの成長は、これらのデバイス、アプリケーション、ネットワーク及びプライバシーとセキュリティの確保に新たなリスクをもたらします。

本書では、ＩｏＴのリスクを形成する三つの要因として「脆弱性」、「意図」、「結果」、リスク評価の三つの指標として、「データの価値」、「機能の重要性」、「故障の拡張性」を挙げ、ＩｏＴのリスクをどのように管理していくかについて記述されており、企業のＩｏＴのリスク管理の一助になるものと思われます。本小冊子が我が国の情報セキュリティ体制の向上にいささかでも貢献できれば幸いです。

平成２９年８月

公益財団法人　防衛基盤整備協会

理事長　鎌田　昭良

# 目　　次

## ＩｏＴのリスク管理

## ＣＳＩＳについて

戦略国際問題研究所（ＣＳＩＳ）は、５０年以上にわたり、世界的政策課題への解決に取り組んできました。今日、ＣＳＩＳの学者は、意思決定者がより良い世界に向かう進路を立案することを援助するために、戦略的洞察力と超党派的な政策案を提供しています。

ＣＳＩＳはワシントンD.C.に本部を置く非営利組織です。研究所の２２０名の常駐スタッフと提携する学者の大きなネットワークは、研究と分析を実施し、将来を見通し、変化を予測するための政策イニシアティブを提供しています。

冷戦の最盛期にデービッドM.アブシャイアとアーレイバーク提督によって設立されたＣＳＩＳは、アメリカの威信と繁栄のために、世界の善の力として貢献してきました。１９６２年以降、ＣＳＩＳは、国防と安全保障、地域の安定、そして、エネルギーや気候から世界的な保健、経済統合までの超国家的課題を専門とする世界で最も著名な国際機関の一つになりました。

２０１５年１１月にトーマス J. プリッカーが、ＣＳＩＳの理事長に任命されました。２０００年からはジョンＪ.ハムレ元米国国防副長官が､研究所長兼最高経営責任者になっています。

ＣＳＩＳは、特定の政策的立場をとっておらず、ここに論述されるすべての意見は、著者の個人的見解であると理解されるべきです。



謝辞
本報告書は、シマンテックコーポレーションの絶大なる支援のもとに完成しました。

戦略国際問題研究所
1616 Rhode Island Avenue, NW
Washington, DC20036
202-887-0200|www.csis.org

## 要　約

インターネットの大多数の「ユーザー」は機械であり人間ではありません。「モノのインターネット（ＩｏＴ)」を構成するデバイスは、インターネットに接続され、作動し、そして莫大な量のデータを創り出します。これらのデバイスは、やがて更なる機能を発揮し、安全とセキュリティにとって新しいリスクを創造しますが、リスクを評価し、有益な政策を考案するためには、逸話以上のものが必要です。セキュリティとＩｏＴ（モノのインターネット）に関する最初の結論は、一般的な描写によってリスクが大きく誇張され、誤って伝えられているということです。

１．ＩｏＴは、通常のインターネットと同じように安全ではなく、より脆弱なものです。なぜなら、多くのＩｏＴデバイスは、限定的な機能を持つ簡単なコンピューターを使用しているからです。
２．脆弱性の増大が、リスクの増大を意味するものではありません。ＩｏＴによる利益は、その潜在的危害よりはるかに大きいのです。あまり考慮されていないリスクの一つは、セキュリティやプライバシーに対する時期尚早または過剰な手段が、経済成長とイノベーションを阻害するということです。
３．ＩｏＴデバイスは、ハッカーが物理的な効果を生み出すことを可能にします。研究者は、ＩｏＴデバイスにおける多くの脆弱性を実証してきましたが、こうした脆弱性の影響は、主に悪質ないたずらだとみなされています。機微な機能を遂行し、あるいは妨害により、大規模な影響を及ぼすようなデバイスのみが、リスクを増大させます。これは、大部分のＩｏＴデバイスが、ほとんどリスクをもたらさないことを意味します。
４．オンラインによるプライバシーは大きな恐怖なので、ＩｏＴがそれを更に悪化させることはありません。
５．サイバー空間の安全を妨害する同様な問題は、ＩｏＴのセキュリティに対する進歩を遅らせます。こうした問題は、技術的な不確実性、限定的な国際協力、改善のためのインセンティブの欠如、限定的な立法権限、オンラインの脆弱な個人識別（ＩＤ)、そして個人データを利用するインターネットのビジネスモデルなどです。
６．サイバーセキュリティのため、通常使用するのと同じアプローチ、すなわち、研究、責任、国際協力及び規制によってリスクの減少を加速することができます。ホワイトハウスは、重要なインフラに対するアプローチを反復し、企業が使用、販売するＩｏＴデバイスに対するセキュリティの改善を図るため、担当機関に、企業と協力するよう任務を付与することができます。
７．自律性は、ＩｏＴリスクのカギとなる決定的な要素です。デバイスに対する自律性の制限や自律性を無効にする方法の提供は、リスクを減少させます。ＩｏＴの基準には、人間による大幅な介入や機微な機能の制御を必要とします。

８．不安全なネットワークに接続された安全なデバイスは、リスクの減少にはつながりません。ほとんどのネットワークでは、セキュリティが弱いので、ＩｏＴをより安全にするためには、ＩｏＴデバイスとネットワークの両方に対する暗号の使用、強力な認証、復元力の増大が必要です。

９．ＩｏＴリスクを評価するために、データの価値、機能の重要性、故障の拡張性という三つの指標を使うことができます。脆弱なデータを創り出し、重要な機能を遂行し、あるいは大規模な効果を生み出すことのできるデバイスは、高度な基準に維持する必要があります。それができないデバイスは、修正のため市場の力や裁判所に委ねることができます。

10．リスクはダイナミックです。リスクは技術が進化し、知識と経験を重ねることによって減少します。ＩｏＴを経験することによってリスクは減少します。

# ＩｏＴのリスク管理

ジェームス・アンドリュー・ルイス

## １．はじめに

ＩｏＴの危険性についての警告は簡単に見つかります。これらの警告は、リスクの性質と、いかにイノベーションが技術をより安全にするかということを誤解しています。

「モノのインターネット」という用語は、計算能力とインターネットアドレスを持つネットワーク化されたデバイスを表現するため、１９９０年代に初めて使用されました。インターネットに関する多くの予言のように、ＩｏＴの発想は未熟なものでしたが、２００８年には、インターネットの「ユーザー」として機械が人間の数を上回るようになりました。これらの機械はワイヤレスで接続され、作動し、データを創り出します。ＩｏＴデバイスは、次第に多くの機能を遂行するようになり、ネットワークにつながれていないデバイスよりも、更に効率的で安価になります。企業や消費者が、既存の製品やサービスを改善したり、新しい製品やサービスを生み出すために、スマートな機械を使用するように、市場の要求によって容赦なくＩｏＴを使用するようになります。

この新しいデジタルネットワーク技術の適用は、スペクトル管理、プライバシー、データの局地化、運用に至るまで多くの政策上の課題を引き起こします。ＩｏＴの利益を最大限にするために必要な政策の枠組みを策定するためには、多くの年月が必要です。本報告は、政策の策定を導く一つの方法として、リスクとそれをいかにして測定するかを検討するものです。

すべての新しい技術にはリスクが伴います。リスクがどれくらい大きいかは別の問題です。個々のＩｏＴデバイスが、攻撃に対して脆弱であるとしても、それが新しい莫大なリスクを意味するものではありません。攻撃者がすべての脆弱性を利用するかどうか（ありえないことですが)、そして脆弱性を利用した結果がどうなるのか、を検討しなければなりません。これらの結果は、悪戯から生命を脅かすものまでありますが、ごくわずかなケースだけが、社会に対する本当のリスクなのです。考慮しなければならないことは、今直面しているサイバーリスクに比較して、どれだけリスクが増大するのか、いかにしてＩｏＴのような新しい技術を使うことによって生じるリスクを、イノベーション、起業家精神、経済成長を損なうことなく管理し、減少させることができるのかということです。

## ２．ＩｏＴとは何か

初期の鉄道は数マイルの線路しかなく、馬より遅い列車でした。一世紀後、広大な鉄道網は、現在の列車や自動車とは程遠い速度で動く複雑な機関車によって米国をカバーしていました。コンピューターデバイスのネットワークに関しては、いまだに２０世紀

の特急列車より馬に近いのです。しかし、列車のように迅速に次々と改善が行われることによって、新しい社会的、経済的な過渡期の環境が整備されつつあります。

列車の例えを続けると、性能が向上したにもかかわらず、「サイエンティフィック・アメリカン」のように威厳のある雑誌でさえも、１９世紀に人間の身体は、時速４５マイル以上のスピードには耐えられないと述べました。知識の欠如や先天的な警戒心によって、新しい技術から出現するリスクは、現実よりも大きいと思うようになるのです。

コンピューターは列車ではありません。コンピューターは思考し、意思決定をするようにみえます。機械がプログラムを実行する速度を考えれば理解は可能ですが、これは大半が幻想です。現在のコンピューターデバイスは、真に自律的なものではありません。しかし、自律的なデバイスの恐怖（映画「ターミネーター」の中で、人間に挑戦する自律したインテリジェンス「スカイネット」を考えてください）が、ＩｏＴの議論には存在します。それは、相互に連接された「考える」機械が、人間の支配者に挑戦し、人間の支配者にとって替わるということが未来には起こるかもしれないという恐怖です。機械が新しい危険を創り出し、人間にとって替わるという恐怖は、産業化時代に始まりましたが、依然として強力で、しかも強烈に間違った恐怖として残っています。ＩｏＴは、人間の能力を拡大する唯一かつ最新の手段であり、産業化の初期に起源をもつ日常的な活動の自動化の最終段階にありますが、ＩｏＴも同様の恐怖をもって歓迎されてきました。

ＩｏＴを構成するデバイスは、通常、IP アドレス、内蔵コンピューター、環境を感知するある種のセンサーをもっており、ほとんどのデバイスが、ネットワークに接続可能（ワイヤレスで接続）です。そのデバイスは、消費財から巨大な産業用機械に至るまであります。ＩｏＴデバイスは、いつ特定の行動をとるか、いつ異なる行動の中から選択するかを、デバイスに「決定」させるプログラムを実行します。ＩｏＴデバイスは、非ＩｏＴデバイスには存在しない脆弱性を持っているかもしれません。

ＩｏＴは多くの日常的な活動を自動化し、それによって機械が、人間の関与なしに意思決定をすることができます。自律的なデバイスは、在庫を統制し、インターネット上の商業契約を認可し、そして人間の介入なしに、船舶への積載や配送を手配します。相互作用は迅速かつ自動的に行われ、ユーザーがアクセスできない構成と性質を持つ事前にプログラムされた一連のルールに従って実行されます。

これらの変化は、生産性の増大とコスト削減によって、計り知れない経済的利益を提供します。このように、ＩｏＴの効果は、１９８０年代、９０年代のビジネスによって広く採用された時代のコンピューター技術による経済的利益として映し出されます。同様にインターネットが初めて商業化されてから、経済学者は「ＩＴ（情報技術）は最近の米国経済における生産性改善の主要な要因である。」と結論づけました。あるアナリストはこう書いています。「ＩＴ（情報技術）についてワクワクすることは、その他の資本にとって代わる能力ではなく、新しいタイプの市場と組織を作るプロセスにおいて、ビ

ジネスのすべての局面を再構築する能力である。コンピューターとインターネットによって提供された生産性の向上は、最近、減速しました。ＩｏＴは、それを回復させる可能性を与えてくれます。

人間のオペレーターがいないデバイスに対し、ネットワーク化されたコンピューターを拡大することは、６０年前の大量のメインフレームコンピューターにより開始された手順における次の段階です。コンピューターは小型化、迅速化し、ネットに接続されて、平凡なものから複雑な機能まで埋め込まれたものになりました。コンピューターデバイスはユビキタス（いつでもどこでも存在する）になり、モバイル（携帯可能）なものになりました。ＩｏＴによる挑戦は、どの機能を、人間が介在しないで作動する機械に移転するかという問題に取り組むことになるので、新しいものです。これらの課題は、経済におけるデータの新しい中心的な役割と（これがプライバシーにとって不安な影響を及ぼすこと）、現在のコンピューターが外部操作から十分に防護されていないというセキュリティの欠陥によって、より複雑になります。経済的な機会と増大したリスクの潜在能力は、ＩｏＴ政策を考える上での背景を提供します。

## ３．ＩｏＴのリスクをいかにして評価するのか

人は、リスクを容認し、管理します。消費者や企業は、リスクに対する寛容さ及び「リスクのある」活動によって得られる価値とリスクの見積りに基づいて意思決定を行います。リスクの認識は、製造者は安全な製品を製造する、基準と規制は生産と使用のためのガイダンスを提供する、もし安全が損なわれた場合に裁判所は救済策を提供する、という安全に関する知識と仮説によって形成されます。

ＩｏＴとリスクに関する懸念には、「９．１１の攻撃」以降の米国社会における様々な変化が反映されています。１９９０年代の輝かしい千年祭ではなく、現在は、デストピア（暗黒郷）として描写される世界です。しかし、ほとんどの手段－平均寿命、死の原因、経済的安定、暴力的紛争の頻発－によって、世界人口に対するリスクは大きく減少しました。そうでなければ、米国の主要な死の原因が、肥満であると主張することはできません。

メディアの報道が、公共の知識と態度を形成します。これはリスクに対する認識をゆがめています。この点において影響力のある作品が、１９８７年にサイエンス誌に発表されたポウル・スロビックの「リスクの認識」です。そのなかにはこう書かれています。

技術的に洗練されたアナリストは、危険を評価するためにリスクアセスメントの手法を使いますが.... 大多数の市民の危険に対する経験は、むしろ不運な事故や脅威を徹底して立証するニュースメディアに基づく傾向があります....

ほとんどの米国人の支配的な認識は、（ほとんどのプロのリスク評価者の意見とは対照的な認識なのですが）過去より現在のほうが多くのリスクに直面し、将来のリスクは現在のものより大きくなるというものです。

それは、サイバーセキュリティの研究者が、いくつかの脆弱性や脅威を発表するための日常的な慣習になっています。そしてこれが、メディアによって取り上げられるようになりました。それは無料の公共財ですが、この慣習がリスクに対する理解をねじ曲げ、文脈なしに個別のケースを取り上げることによってリスクを誇張しています。逸話が分析にとって代わるのです。価値があるのは、実際の結果に対する評価です。

ＩｏＴにとって、何十億ものＩｏＴデバイスが利用されていますが、それらのデバイスに起因する死亡事故は、一件もありません。ＩｏＴデバイスの利用が拡大し、ＩｏＴデバイスの機能がより進化するにつれて、これは変化するかもしれません。現在では、リスクがあるかないかによって、ＩｏＴに対するアプローチの背景を形成すべきなのです。

自動車は、ＩｏＴが如何にしてリスクを作り変えるのかを示すよい事例です。自動車の衝突は、通常、運転者のミスによって起こります。衝突の中には、装置の故障によって、あるいはあまりないことですが、設計や製造上の欠陥によって起こることもあります。誰も自動車の衝突に巻き込まれることを望んではいません。製造者が、リスクの軽減措置を取ることを期待しています。

多くの研究者は、自動車をハッキングすることは可能であり、仮説として、発見された脆弱性が、衝突を引き起こすために使用されることを示しています。極端なシナリオは、ハッカーが、ブレーキシステムや加速システムを乗っ取ることができ、高速走行中にエンジンを停止させることができるというものです。こうした事例は、人の興味を引くものではありますが、結論ではありません。最初の疑問は、ハッキングによる衝突の数が、ＩｏＴ車両によって防止された衝突の数より大きいかどうかということです。もしＩｏＴが、ハッカーの起こす衝突よりも多くの衝突を防止することができるなら、それは社会にとって大きな利益です。ほとんどすべての自動車の衝突には、運転者のエラーが介在するので、半自律的な自動車は、運転者のエラーを低減し、自動車事故の数を減少させ、社会に対する最終利益がリスクより大きいというのが、現実的な仮説です。

イノベーションによって、自動車や他のＩｏＴデバイスのハッキングの可能性と結果が減少するので、リスクは減少します。こうしたイノベーションは、進化し続ける可能性が高く、次々に出る車種は、以前の車種より安全です。２０年前に作られた自動車と、現在の自動車の安全上の相違は大きく、同様にコネクティッドカー（自動運転自動車）やＩｏＴデバイスについても同じ進化のプロセスを期待することもできます。規制によってこうしたイノベーションを加速することができますが、過度の規制は、決定にあたって考慮すべきリスクを伴います。規制は、ビジネスの決定や投資を変化させます。通常、規制はいい方向に向かうのですが、不必要な規制によって、機会と成長を不必要に削減する社会的コストを課すこともできます。

いかにしてＩｏＴリスクを管理すればよいのかを考える上で、自動車の事例は役に立ちます。自動車には多くの小さなコンピューターが搭載されており、そのコンピューターの中には、ハッキングに対して脆弱なものもありますが、重大な懸念になるようなシ

ステムはほとんどありません。自動車の走行を制御する重要な機能に対するアクセスが、リスクを発生させます。搭載されたエンターテインメントシステム（ワイヤレスでインターネットに連接される）に対するアクセスは、システムが、重要な機能に連接されたときのみにリスクを発生させます。自動車のハッキングは、重要な機能が操られたときのみリスクが増大します。コンピューターが故障しても走行できるよう自動車がいかにして設計されているのかがリスクを決定します。つまり、ＩｏＴシステムの機能が低下しても走行を継続できる車は安全なのです。

衝突回避や走行レーンを維持する機能を自動的に行う半自律的な自動車はより安全になります。同時に、インターネットに接続された半自律的な自動車には脆弱性の増大が伴います。こうした脆弱性はリスクの増大を意味します。公共政策上の問題は、いかにして悪い結果に対する社会的コストを、イノベーションや合理的な自由に対するコストを伴わない手段によって削減するのかを問うことです。リスクを減少させる「手段」は、規制、製品の改善、訴訟です。

自動車は、ハッキングに対して脆弱なので、安全ではないことが公表されるなら、製造者は訴訟リスク、責任コスト、（実体的な）ブランドダメージを検討します。製造者の決定は、規制当局が安全なＩｏＴ自動車の基準を作成する能力に依存します。規制のインセンティブと市場の力（責任を含む）の組み合わせを通じ、自動車会社は劇的に安全な車を作りました。１９２１年、米国では百万マイル走行毎に２４件の死亡事故が発生しました。２０１３年までに、死亡事故の件数は、設計・技術上の改善が規制と組み合わせられることによって百万マイル走行毎につき１件程度までに削減されました。事故の件数は減少し続けています。

社会は、これらの同じ手段をＩｏＴにも適用することができます。ＩｏＴは、３種類のリスクを創り出します。それは、ＩｏＴデバイスは故障する、ＩｏＴデバイスはハッキングされる、プライバシーの保護やＩｏＴをより安全にする努力は、リスクの減少を上回る経済的損失を生み出すということです。保険会社は、どのくらいの頻度で事故が発生するのか、それにはどのくらいのコストがかかるのかを示す保険データや歴史的記録を使用してリスクを計算します。ＩｏＴを含めたサイバーセキュリティには、ほとんど保険上のデータはありません。これは正確なリスクの予測を困難にしますが、リスクの方程式を形成する要因を定義することはできます。

脆弱性：攻撃者がコンピューターデバイスに対するアクセスと制御を獲得する能力。攻撃者がデータを操作または抽出する能力。攻撃者がサービスを制御または妨害する能力。ほとんどの研究者は、多くのＩｏＴコンピューターデバイスには技術的な限界があるので、ＩｏＴに使用されるコンピューターデバイスはよく知られたインターネット技術よりも脆弱であると信じています。これらのデバイスの多くは、これまでのデスクトップやラップトップが持つ伝統的なセキュリティ機能を遂行する能力が欠如しているので簡単に標的にされます。

意図：ＩｏＴデバイスが、ただ単に脆弱であるからと言って悪意のある目的のために誰かがそれを利用するということではありません。攻撃者は、攻撃が政治的、軍事的、経済的、社会的利益を提供できるかどうかを計算した上で、脆弱性を利用するかどうかを決定しなければなりません。意図は、単純な敵意、犯罪、スパイ、テロリズム、戦争をすべて反映することができます。これらはすべてサイバーセキュリティでみられる通常の動機です。

結果：コンピューターデバイスは脆弱で、攻撃者がこれらの脆弱性を利用するかもしれませんが、最終的な問題は「それがどうした、利用されてもいいじゃないか。」ということにあります。すでに、社会には、ハイレベルな暴力、犯罪、事故が起きていますが、社会は、これらを吸収する驚くべき能力をもっています。ＩｏＴデバイスにみられる脆弱性のほとんどは、悪戯とみなされる事件に結びつきます。より大きな問題は、ＩｏＴが、生命の損失や重大な経済的損害につながるようなシステム的脆弱性をもたらすかどうかです。

脆弱性、意図、結果によって、ＩｏＴの事件による被害確率を見積もることができます。ほとんどの分析は、実証可能な脆弱性の高さに焦点が当てられています。これは、リスクを予測する上で最も重要な変数ではありません。脆弱なデバイス、悪意のあるアクター、潜在的に損害を引き起こす結果の組合せによって生起するリスクを見積もるため、損害を引き起こす結果を創り出す脆弱性を利用した悪意のある行動が、いかにして生起するのかを検討する必要があります。リスクを評価する仕事の一つは、ＩｏＴデバイスの総数を分析し、機能の重要性や攻撃の拡張性によって、真のリスクが存在するデバイスを分類することです。最大のリスクは、重要な機能と脆弱なデバイスの交点に存在します。

出発点は、ＩｏＴが他のインターネット技術と同様に安全ではないと仮定することです。いくつかのケースでは、他の技術ほど安全ではありません。最近２０年間の経験によって、安全なコード（符号）を書くことがいかに困難かを示しています。ＩｏＴデバイスの進化は更なる脆弱性を生み出します。多くのＩｏＴデバイスには、ソフトウエアを修正し、アップグレードする限定的な能力しかありません。多くのＩｏＴデバイスは認証、暗号の管理に対する困難に直面しています。より進化したデバイスは、セキュリティ機能をよりよく遂行することができますが、これらのオプションには、付加的なコストや消費者レベルにおいては、そうした要求が少なくなるという複雑さがあります。デバイスに対する性能上の制限は、ＩｏＴを安全にする能力を抑制します。

多くのＩｏＴデバイスは、消費財です。消費者用ＩｏＴデバイスのハッキングが、重大な損害を引き起こすというシナリオは、ますます疑わしくなっています。なぜなら、消費者用ＩｏＴデバイスのハッキングは、局地的かつ一時的な効果しか生み出さないというもっともらしい状況があるからです。冷蔵庫の電源を切ることは、牛乳をダメにする原因ですが、乳牛、酪農業者、食料品店に対して、付加的なストレスを与えます。攻

撃は行われますが、これはそんなに驚くことではありません。

極端な例ですが、もし、ハッカーが墜落につながる重要な航空機システムを制御することができるなら、その効果はテロリストの爆弾に匹敵するものになります。しかし、これは航空機の乗務員が制御を回復できないことを前提としています。直接的な予防方法は、乗務員にＩｏＴシステムを無効にする能力、あるいは、基本的な運航体制にリセットする能力を確保させることです。航空機などに現在使用されている多くのデバイスは、構成部品の故障に対応するように設計されています。また、パイロット訓練プログラムには、故障対処が取り込まれています。同様に、エレベーターをコントロールするためには、最新のエレベーターに使用されている３～４つの機械的な安全システムを破ることが必要です。

ＩｏＴ攻撃の反復性は心理的なインパクトを決定します。反復され、止めることのできないハッキングは、自爆攻撃が長期戦争の発端かどうか不明であった「９．１１」以降に米国で蔓延したものと同様の恐怖や不確実性を創り出します。航空機の墜落を起こす能力は恐怖になりますが、これらの事故が、いつ、どの程度繰り返されるのかを予言することは難しいので、その恐怖は増大します。

ＩｏＴの脆弱性に対するほとんどの説明は、一つのハッキング事件が大規模なスケールで再現される可能性があると想定していますが、ほとんどの場合、課題は１台の車や冷蔵庫をハッキングすることではなく、大規模な効果を生み出す状況や環境において、数千というハッキングを行うことだと仮定しています。このような大規模な事件に介在する変数の数は、このようなハッキング事件がほとんど起こらないことを示唆しています。ハッカーが理想的な条件の下で一つのデバイスに故障を引き起こし、それが安全やセキュリティに対してより大きな脅威となるような一つの事例から全体を推定することを誰も望みません。現代の経済が、正常として受け入れている不協和音や混乱の平均レベルは高いのです。ＩｏＴのハッキングが目立つようになるには、この敷居を超えなければなりません。

ほとんどのＩｏＴデバイスは、重要な機能を遂行することはなく、重要なデータを生成し、蓄積することもありません。これは、特に消費者用ＩｏＴデバイスにとっては真実です。これは、消費者用デバイスがたとえハッキングされたとしても、その結果は、ほとんどが迷惑程度になることを意味します。悪戯に大きく晒される国家は、大きなリスクには直面しません。それは全身を侵すリスクです。すなわち、一つの決定的なノード（ＦｅＤｗｉｒｅ:連邦準備銀行の即時グロス決済資金移動システム、電力網、原子力発電所のような）を攻撃すること、あるいは、物凄い数の目標を同時に攻撃することによって、重大な効果を発生させる能力です。簡単な予防策は、リスクをよりよく評価し、コントロールできるようになるまで、インターネットに接続されていない重要なシステムを接続しないままにしておくことです。

## ４．ＩｏＴと大規模な効果

ＩｏＴ攻撃のリスクを大幅に増大させるためには、拡張性を持たなければなりません。ＩｏＴデバイスのハッキングによる全身的、大規模な効果は、二つの条件によって決定されます。それは、他のデバイスを支配する一つのデバイスをハッキングする能力（時には単一障害点として知られる）、もう一つは多くのデバイスを同時にハッキングする能力です。誰かを殺害するためにブレーキに細工をすることは、映画のメロドラマの定番ですが、自動車のブレーキをハッキングすることは、悪意のある悪戯かまたは犯罪なのです。同時に何百台という自動車をハッキングすることは、リスクを増大させる大規模な効果になります。

この大規模な効果の敷居は高いのです。例えば、２０１３年に米国では、３０，０５７件の致命的な衝突事故が発生し、毎日平均８５名の人が交通事故で亡くなっています。事故は悲劇的で、何人にも望まれず、代償が高くつくものですが、これは社会に対して有害な影響を及ぼしません。ハイウェイを走行中に自動車のエンジンを停止させることは、（速度やその他の要因にもよりますが）運転者にとっては致命的で、交通を混乱させますが、大規模な効果は生み出しません。

ハッキング可能なＩｏＴデバイスは、ハッカーに乗っ取られたコンピューターデバイスである巨大な「ボットネット」を作るために使用され、ＤＤｏＳ攻撃の目標を攻撃するためのトラフィック（通信量）を生み出すために使用されることもあります。ＩｏＴはデバイスの人口を増加させますが、ＤＤｏＳの話は、攻撃の規模を継続的に増大させる攻撃側と、攻撃をそらせる方法を見つける防御側の話です。この防御側と攻撃側のいたちごっこは、より多くのＩｏＴデバイスが、オンライン化されるため継続します。ＤＤｏＳ攻撃は進化しますが、同様に防御も進化します。ボットネットはもはや驚くべきことではないのです。

悲劇的なリスクは、ＩｏＴデバイスに対する悪意のある攻撃が、大量の死者や大きな経済損失を引き起こすような事件の蓋然性です。悲劇は、脅威に対して過度に使用される言葉で、幸運なことに、米国は歴史上二つの悲劇的な攻撃しか経験していません。それはパールハーバー（真珠湾攻撃）と９．１１です。核兵器は悲劇的な効果を生み出しますが、サイバー攻撃は、核兵器の爆発と放射線効果を再現することはありません。

「サイバー９．１１」は、現実的なシナリオではありません。テロリストは、ハッキングでは不可能な暴力行為の衝撃的価値をよく認識しています。９．１１の全体コストの見積もりには様々なものがありますが、ある見積もりでは、攻撃のコストが物理的な破壊で５５０億ドル、経済的影響で１２３０億ドルだったとしています。 ３０００人以上の人命損失のコストは見積もることができません。社会的、経済的な「アフターショック」は同様に相当なもので、物理的破壊と経済的影響で、１８８０億ドルとされていますが、この中には国土安全保障経費の激増や経済活動妨害の間接的経費は含まれていません。自動車やトースターのハッキングは、たとえ、何千とハッキングされようと、

９．１１と同様の衝撃と損害を与えることはありません。

ＩｏＴに対する危険なハッキングのより現実的な比較は、２００３年の北東部大規模停電との比較です。この停電は、推定６０億ドルの損失（多くは生産損失）であり、１１人の死亡者発生の原因になりました。ＩｏＴシステムに対して周到に計画され実行された攻撃は、同様の効果を生みだすことができます。大きなネットワークを制御して、防護機能を持たない何千もの家庭のエアコンシステムを、一日のうちで使用時間の多い時間帯に最大出力となるように同時に細工をすることができれば、それは電圧低下や停電を引き起こします。

サイバー攻撃に対する電力網の脆弱性は、１０年以上にわたり話題となってきました。電力網をより安全にするいくつかの進歩も見られましたが、それは均質ではありませんでした。電力網に存在する脆弱性に関して、ＩｏＴは新しい種類の脆弱性を生み出しますが、それによってどれだけ多くのリスクが増大したかは、ＩｏＴデバイスがどのように設計され使用されるかに依存しています。

例えば、英国では、一部のスマートメーターに電力網から世帯を切断することができるメカニズムが含まれていて、電力会社がこれらのメカニズムを制御しています。誰もが同じソフトウエアを使用するため、ハッカーは、悪意のあるコードを挿入し、同時に何千ものメーターを切断することによって、コミュニティ全体の電力を停止させます。更に、迅速な修理を妨害するため電力ユーティリティとインターネットの接続を不能にすることができます。同様に、カルフォルニア州では、消費者によるセッティングの変更ができず、サーモスタットの遠隔操作によってセッティングを変更できるスマートグリッドデバイス（ＰＣＴ：プログラム通信サーモスタットと呼ばれる）を要求しています。ハッカーは、この特徴を利用することができます。これらは、設計による欠陥です。なぜなら、これらのシナリオでは、人間が介入する余地が制限されており、こうした制限によって、ハッカーがユーティリティや消費者が簡単に修理できない停電を引き起こすことができるからです。そのような事件の効果を評価するためには、サイバーセキュリティリスクでは、計算にない二つの要因を考慮しなければなりません。社会には、復元力や反応力があります。これらの要因は、サイバーセキュリティリスクの見積りではほとんどいつも過小評価されています。人は、損害があれば反応し修復します。社会は、予想以上により多くの罰を吸収することができます。故障の範囲を減少させる選択肢や回避策もあります。社会は反応力があり、大きなＩｏＴ事件や繰り返される小さな事件は、変化や改善につながります。

攻撃者は、急速に大規模な攻撃を起こすことによって復元力や反応力に打ち勝つことができます。しかし、大規模な攻撃は、ほとんどのハッカーの能力を超えているため困難です。今までのＩｏＴデバイスに対する攻撃実験の結果、影響を受けたのは、個人システムのみでした。ＩｏＴ技術の性質を考えれば、大規模なスケールのハッキングには大きな資源と計画能力が必要です。国家がそのような能力を保有していますが、主要な

テロリスト事件に匹敵するようなＩｏＴの戦略的効果を成功と定義すれば、これは成功を保障するものではありません。

邪悪で天才的なハッカーは銀行強盗をしますが、社会に大惨事をもたらす策略のためには時間を無駄にすることはありません。軍事政策立案者は迅速な効果を望み、敵に勝つためには、反復攻撃が必要なことを認識しています。テロリストは、ドラマと流血を望みます。大雑把に言えば、ハリウッドのスリラー映画の陰謀のようなものが増えれば増えるほど、益々それが起こる可能性は少なくなります。これは、大規模攻撃や重要なシステムに対する攻撃を除いては、ＩｏＴリスクの増大は少ない、ということを意味しています。

## ５．意図の問題

ＩｏＴが、潜在的攻撃者の利用しそうな妨害の機会を作るかどうかを評価にするにあたり、最も重要な要因は脆弱性ではなくその意図です。意図は脆弱なデバイスがいかにしてリスクを増大させるかを理解するため決定的に重要です。ＩｏＴの脆弱性によって悪意のある行動が生起する機会は増加しますが、これは、意図がなければ全ての機会が利用されることはないということです。サイバー空間における悪意のある事件の頻度を見ることによってＩｏＴリスクを見通すことができます。最近１５年間で、何千件ものサイバースパイやサイバー犯罪の事件が起きており、このうち何十件かが、強制的行為（国家又は国家の代理である非国家グループが､ネットワークやデータを妨害してきた）で、おそらく数件の事件が物理的な損害や破壊を起こすものでした。こうした有害な事件は、インターネットが数億から数十億のユーザーに拡大したために起こりました。現在までＩｏＴ事件は起こっていませんが、それでもＩｏＴデバイスの数は、数十億にのぼっています。

この期間、大規模なサイバー妨害事件が日常的に予測されてきましたが、一度も起こっていません。広範かつ頻繁に利用される脆弱性にもかかわらず、サイバー事件は、経済的利益や国際政治によって大きく予測可能なものになりました。脆弱性は、攻撃に対する良い予言者ではありません。ほとんどのデジタルデバイスが脆弱である現在の状況では、こうした脆弱性は、通常、犯罪やスパイ行為に利用されますが、物理的損害を起こすために利用されることはほとんどありません。

今ここで評価しようとしていることは、米国におけるサイバーに依存するインフラとサービスがサイバー攻撃に対して脆弱であるかどうかではなく、ＩｏＴがどれだけこの脆弱性を増大させるかなのです。こうしたＩｏＴのハッキングは、サイバー攻撃のもう一つの変形としてみなさなければならないのです。ＩｏＴは、敵がサイバー攻撃で選択する目標の数とタイプを増加させますが、いつ、そのような攻撃を行うかという敵の意思決定プロセスは、ＩｏＴがあっても変わることはありません。

敵対国は､政治的な強制のためにＩｏＴの脆弱性を利用しようとするかも知れません。

ソニーとラスベガスサンズ(Ｓａｎｄｓ　Ｌｏｓ　Ｖｅｇａｓ)に対するハッキングは、米国人個人に懲罰を与えるための北朝鮮とイランの行動でした。国家規模のハッカーは、ＩｏＴデバイスの妨害によって、懲罰のため個人を目標にすることができます。それは、喜劇から悲劇に至るまでの効果をもたらします。国家による本当のサイバー攻撃（強制または損害を与える意思を持つ。）は、武力紛争の時にしか行われません。米国との武力紛争の場合には、敵対国はＩｏＴを使う重要なインフラを妨害したいと考えるかもしれません。しかし、いかなる種類の兵器（ミサイル、航空機、コマンドー）を使って米国を攻撃するのかという同じ抑制が、ＩｏＴデバイスへの攻撃を含むサイバー攻撃にも適用できます。国家は紛争の拡大や報復を招くことを望んではいません。

攻撃者は、国内のインフラに対する攻撃が、米国との紛争に拡大するのではないかと危惧し、それを局地化することを望むかも知れません。電力網のような重要なインフラを妨害することは、拡大の危険性と米国から破壊的な対応を受けるリスクを冒すことになります。金融システムのような一部のシステムを妨害することは、攻撃者にとって報復のリスクが増大するのと同様に、損害を被るような反響がおこるかもしれません。例えば、南シナ海をめぐる衝突では、中国は紛争を局地的に封じ込めることを好むかもしれません。それがたとえ局地的、短期的な紛争であっても、ＩｏＴシステムに対する攻撃が軍事的優位を与えるかどうかは明らかではありません。大規模な動員を伴うグローバルな長期紛争、例えば、第２次世界大戦の再現のようなシナリオは排除すべきです。なぜなら、このような長期戦争は、出費やリスクの面からすればあり得ないからです。

確かにＩｏＴが、強制やテロの目的に使用されるというシナリオもいくつかあります。（当分の間、テロリストにその能力があるかどうかは別として）テロリストは、ＩｏＴの脆弱性を利用した攻撃を考えるかもしれません。テロリストは、地下鉄を爆破する代わりに列車の衝突を起こすことができます。しかし、テロリストに対してサイバー攻撃の使用を抑制したものと同じ抑制が、ＩｏＴの脆弱性を利用した攻撃にも当てはまります。もし、テロリストが、大規模な混乱を引き起こすシナリオを発見し、それを実行するならば、ＩｏＴに対するハッキングは、テロリストにとって魅力的なものになりますが、テロリストには、直接行動、流血、政治ドラマを好むという心理的欲求があります。ハッキングは、物理的攻撃と同じ程度まで、これらの欲求を満たすことはありません。

政治活動家は、声明を発表するために、ＩｏＴデバイスを妨害することができます。活動家は、ウエブサイトの外観を損なう代わりに、不安を創り出すことができるかもしれません。セキュリティの弱い多くのコンピューターデバイスをインターネットに接続することは、ボットネットの規模や数を増大させる機会を創り出します。全部ではありませんが、ＤＤｏＳ攻撃の多くは政治的行動を好みます。匿名の侮辱をネットに投稿するインターネットトロール（インターネット荒らし）は、物事を一歩進めて、自動車や家庭用品を妨害するかもしれません。ここでの問題（テロリストや国家による強制）は、標的が二つのカテゴリーに区分されるということです。それは、個人的、政治的効果の

ために攻撃される個人の標的と戦略的効果を引き起こす広範な組織的攻撃です。

## ６．自律性とリスク

スマートグリッドの事例にみられるように、ＩｏＴの自律性に対して適切なレベルを決定することは、セキュリティの基本的な問題です。自律的な作動と人間の制御のバランスによってＩｏＴリスクは形成されます。これを考える簡単な方法は、（運転者のいない自動車のように）ＩｏＴデバイスが人間にとって代わるか、あるいは（スマートカーのようにブレーキや衝突回避を自動的に行うことで運転者を支援するように）人間を強化するかということを検討することです。自律的なＩｏＴデバイスは、作動中いかにあるべきかという論争が、コンピューターに関する議論が行われた初期の時代から続いています。一部の科学者は、コンピューターを人間の能力を増強するものとみなしていたし、他の科学者は、コンピューターが人間にとって代わるものとみなしていました。
多くの人は、既にビデオゲームで自律的なコンピューターデバイスと関係をもっています。ビデオゲームの中では、コンピューターが創り出した「敵」は人の行動を「感知」し、いかに対応するかを決定します。これは、ソフトウエアを実行し、事前にプログラムされた選択肢のメニューに基づき、人の動きに対応して行動をとるゲームボックス内の強力なコンピューターチップスによって行われます。これは 1/1000 秒単位で行われます。その結果は、敵が思考し、環境と関係を持つという幻想です。現実の世界は、より多くのインプットと複雑なプログラミングを必要とする人工的なゲーム環境よりもずっと複雑です。しかし、ビデオゲームは、自律的デバイスの潜在能力を示しており、自律的システムを作るためのテンプレートを創り出します。ビデオゲームにおけるグラフィックチップの大手メーカーの一つであるエヌビディア（ＮＶＩＤＩＡ）社が、モバイルコンピューターと自動運転自動車のチップの重要な供給者になっていることは、興味深い話です。

ＩｏＴデバイスにどの程度の独立性を付与すべきかを決定することは、リスクに関する決定にかかっています。自動車の事例として、車が道路を下り、自動走行していますが、ドライバーは実験に気を取られているとします。緊急事態は、ドライバーが突然に自動車を制御することを要求します。航空機の自動操縦装置は、経験的に機械から人間の制御への突然の移行がリスクを創り出すことを示唆しています。パイロットは、航空機を飛行させるためコンピューターに依存しています。そして十分に状況を把握することなく、突然に決断しなければなりません。更に、自動操縦の経験は、リスクは時間がたてば増大することを示しています。人は自動操縦装置に慣れており、ドライバーやパイロットのスキルは使用しないことによって低下します。ドライバー（又はパイロット）は迅速に反応する必要があるばかりではなく、何をすべきかを知り、それを経験することが必要です。

自律的システムにどれだけの制御を与えるかは、シナリオに依存します。突発的で予

期せぬ変化の可能性が高いのであれば、自律的デバイスは、効果的に対応することはできません。人間のオペレーターが優先的に制御することができ、機械の制御を解除することができる場合、リスクは大幅に減少します。例えば、有人飛行機については、もしパイロットが危険な飛行機の運動をタイムリーに修正することができるなら、リスクは最小限にすることができます。人間の介在を確保し、自律的機能を制限することによって、あるいは、人間のオペレーターがどこで制御から安全に解放されるかを検討することによって、リスクを管理することができます。

これは、ＩｏＴデバイスの信頼性と安全性により自信を持つことができるまでは、重要なサービスを提供し、大規模な効果を引き起こすシステムに対するマニュアルコントロールができるように、システム設計することが重要であることを示唆しています。消費者に自動運転を解除する権限を与えることは、ＩｏＴの経済的利益を減少させると反対することは正しいのですが、大規模な効果や重要な機能を創り出すＩｏＴデバイスの比較的小さなセットにとっては、リスクが増大するため、これが正当化されています。

自律的システムが、人間に追いつき、人間と競争し、最後は人間にとって替わるというリスクに対しては、長年にわたり重大な懸念があります。そのようなシステムに対する進歩は、コンピューターがプログラムによって作動するのではなく、人間のように考えるという人工知能の開発に関する偶発的なものであり、現在では、ＩｏＴによるセキュリティ上の課題はデータを保護し、不当なアクセスや制御を防止するという平凡なものになっています。

## ７．ＩｏＴリスク管理の認証と暗号化

ＩｏＴの安全を技術的に解決するためには、暗号化と強力なＩＤ認証が必要です。暗号化の多用と認証機能の改善は、すべてのインターネットアプリケーションにおけるプライバシーとセキュリティに対するリスクを減少させます。しかし、暗号化と認証の採用は、ＩｏＴのみならず、すべてのインターネット活動にとって、これまで困難な課題となっていました。

ＩｏＴは、データとネットワークの保護において現在直面している最も重要な問題－知的財産、機微なビジネス情報及び個人情報の窃取につながるデータの漏洩－を変化させることはありません。ほとんどのＩｏＴデバイスには、知的財産や機微なビジネスデータは蓄積されていないので、ＩｏＴにとってデータの窃取は大きな問題ではありません。

ＩｏＴデバイスは、個人の行動に関する新しいデータを大量に創り出します。ＩｏＴ技術の導入は、プライバシーのための暫定的なものです。米国は、プライバシーと引き換えに、インターネットサービスの爆発的な成長を獲得しました。西欧は、１９８０年代のプライバシーを維持するという異なった選択をしましたが、かわりに１９８０年代のインターネット経済を手に入れました。米国の消費者は、インターネットが商業化さ

れる前と同様に、今日でも自分の個人データを管理することができません。インターネットのビジネスモデルは、個人データを抽出し、多くのデータと照合して商業のために使用することです。消費者はこれをサービスに対する暗黙の了解として受け入れました。インターネットは消費者の好みと行動を変えました。ＩｏＴは、この個人データを更に生成、収集、蓄積します。企業は製品やサービスを改善し、収益増加のためにＩｏＴデバイスからデータを収集します。ＩｏＴは、量的に新しい種類のデータを生み出しますが、このデータの多くは（例えばタイヤの空気圧や冷蔵庫の温度など）ほとんど価値がありません。しかし、あまり重要ではないデータでさえも、分析目的のために収集され、他のデータと照合させると有益なものになります。一般的に、ほとんどのＩｏＴデータは、集積、分析されたとしてもプライバシーやセキュリティにとってほとんどリスクとはなりません。

サイバーセキュリティにとって認証の弱さは大きな問題です。これまでユーザーの行動や既存の技術は、簡単に修正できないと言われてきました。ＩＤを模倣し、不正に信任を獲得するのは簡単で、それによって侵入者はネットワークやデバイスを制御することができます。ＩＤ認証（一般に認可と呼ばれる）はコマンドの正当性を立証します。消費者や企業による利便性と信頼性の要求によって、強力な認証技術の使用が制限されてきたため、オンライン認証は脆弱です。人は、複雑な手順ではなく迅速なアクセスを望みます。これが、数秒で解読されるパスワードを、今でも使用している理由です。同様な利便性と信頼性の好みが、ＩｏＴデバイスにも当てはまります。人のために働かないものは、ＩｏＴのためにも働きません。ＩｏＴでは、アップデートや修正に偽装した悪意のあるコード（符号）を受け取り、正当で信頼できるソースであるとして、額面どおり容認します。しかし、強力な認証技術は、多くのＩｏＴデバイスで使用される限定的な記憶・処理能力しか持たない簡単なコンピューターのために設計されたものではありませんでした。初期世代のＩｏＴデバイスは、時代遅れの認証に依存し続けているので脆弱です。米国では、１０年以上にわたり強力な暗号化製品を購入することはできましたが、それを使用する人は、ほとんどいませんでした。使用する人にとっては、実行上の問題があり、しかも、暗号化製品の中には簡単に利用されるという基本的な欠陥があります。アップルやＧメールが、自分でするより簡単にメッセージを暗号化してくれるように、暗号化は、サービス提供者によってそれが集中的に提供されたときに効力を発揮します。暗号化は、誰でもが読める平文を、文字と記号の組み合わせに変換します。強力な暗号化（解読が困難か、不可能を意味する）のためには、更なるコンピューターリソース（ＩｏＴデバイスでは供給が制限されている）とＩｏＴデバイスの通信を暗号化し、解読するために使用される暗号鍵（鍵とは暗号化されたメッセージを平文にするためのフレーズやトークン、逆も同じ）を管理する方法が必要です。暗号化プログラムは簡単には書けません。ＩｏＴにとって暗号化は、多くのデバイスがシンプルで、モバイルそしてワイヤレス接続（簡単に傍受される）であるために、特別な課題となってい

ます。もし、ＩｏＴが、人間のインターネットのパターンを踏襲するならば、人は暗号化を使用するために特別な努力はしませんし、デバイスが安全に設計されることもありません。

すべてではありませんが、一部のＩｏＴ機能には、安全のために暗号化されるデータとコマンドの両方が必要です。暗号化に対する通常の解決策は、公開鍵インフラ（ＰＫＩ）と公開鍵暗号基盤（ＨＴＴＰＳにより規定されたＳＳＬやＴＬＳ）です。ＰＫＩは安全に暗号鍵を交換する方法で、暗号化や暗号解読の鍵を交換することを、見知らぬ人に許可する鍵管理の方法です。大きな産業用ＩｏＴデバイスにとって、既存の暗号化製品を使用することは可能ですが、簡単なデバイスにとっては、より小さな記憶・処理能力しか持たない軽量の暗号化を作る必要があります。

ＳＳＬは、ウエブサイトの安全を図るために広く使用される暗号化技術です。ＳＳＬは非脆弱ではありませんが、多くの消費者や商業活動のため、十分なレベルのセキュリティを提供します。ＴＬＳはＳＳＬの改良型です。ＳＳＬとＴＬＳは、安全な認証を提供することができますが、認証技術は、オンボードのＩｏＴの暗号化よりも急速に改善されています。これは、ＩｏＴに必要な戦略はＩｏＴ第一のための認証と認可を強化することが焦点となることを示唆しています。今後数年のうちに新たな認証技術が市場で利用可能となります。それらの技術は、ＩｏＴデバイスにアクセスし、コマンドの発行を求めるデバイスを安全に識別するために、スマートフォン、クラウドに基づいたデータ分析、行動パターン、生体認証などのいろいろな組み合わせを使用します。

暗号化データ、アクセス、制御機能は、セキュリティを増加させますが、かなりの代償を払う必要があります。暗号化は、更なるコンピューターリソース（ＩｏＴデバイスにとっては供給が制限される）を必要とします。暗号化には、同様に「鍵の管理」が必要です。それは、通信を暗号化し、解読するために使用される暗号鍵を管理する方法です。鍵の管理は、特に大規模に行う場合には困難で費用がかかります。ＩｏＴの設計者にとっては、オンボードの暗号化は、コストと複雑性が増えるため魅力的なものではありません。これは、限定的な演算・記憶・処理能力しか持たない消費者用デバイスにとってみれば特に切実な問題です。ＩｏＴの産業用アプリ（消費者用デバイスよりも数は少ないが、経済的にはより大きな価値を生み出す）は、大きな機械なので同じ制限には直面しません。ネットワークにおける暗号化（デバイスの暗号化）は、面倒で非効果的です。ＩｏＴの暗号化のためには、コンピューター的にはそんなに強くない暗号化プログラムの開発とＩｏＴの暗号化をより簡単､安全に展開できる研究開発が更に必要です。これは、おそらく国立標準技術研究所（ＮＩＳＴ）が実施するような基準の設定プロセスが、ＩｏＴデバイスの機能とコストに対する適切な要求を開発することのできる分野です。

ＩｏＴの暗号化のためには、コンピューター的にはあまり強力ではない暗号化プログラムの開発と暗号化をオフデバイスで行うＩｏＴのネットワークを設計することが必要

ですが､更にＩｏＴの暗号化をより簡単､安全に展開できる研究開発が必要となります。データと機能を暗号化することの難しさは、ＩｏＴ市場にとっては妨害となります。すべてのＩｏＴデバイスが、強力な暗号化を使用するという包括的な要求は、すべてのＩｏＴデバイスと機能にとっては意味をなさないだろうし、更に、データや機能の価値と機密性を考慮する必要があります。

## ８．ＩｏＴリスクの管理

ＩｏＴは新しいものですが、インターネットも同様に新しいものです。インターネットは２０年前に商業化されました。その当時は、せいぜい４０００万人しか使用していませんでしたが、現在では、インターネットのユーザーは３０億を超え、９０億のデバイスがインターネットに接続されています。過去２０年間でインターネットから学んだことの一つは、それが利益とリスクの両方を生み出し、利益のほうがリスクより優っているということです。この同じ教訓がＩｏＴのセキュリティに適用されています。ＩｏＴのセキュリティの多くは、デバイスの脆弱性とＩｏＴデバイスの強化の必要性に焦点が当てられています。この戦略の価値には限界があります。ＩｏＴのセキュリティについて異なる方法で考え、ＩｏＴリスク管理戦略の主要な要素として、脅威の環境、自律性の度合い、ＩｏＴネットワークのアーキテクチャーを見ることは有益です。

脆弱性は、リスクに対する良い予言者ではありません。ただ単に、デバイスが脆弱だからといってハッキングされ、損害を引き起こすような結果を生み出すことはありません。今日では、ＩｏＴのリスクは、ほとんど仮説のままです。ＩｏＴデバイスの数と種類が増加するので、これは変わるかもしれませんが、安全や効率の増加と比較し、検討する必要があります。

最初のインターネットでは､低コストによる利益やより多くの成果を獲得するために、ビジネス慣習をデジタル化するという発想に対し、全く疑問はありませんでした。しかし、リスクに対する公共の認識は、悪意のあるサイバー事件の数と範囲を十分に認識することにより変化しつつあります。こうした認識の変化は、ＩｏＴに対する個人的決定や公共の政策を再形成する力を生み出します。

## ９．ビジネスの決定とリスク管理のための政府の行動

ＩｏＴに関しては、ＩｏＴが異なる産業や製品に対して、平等に適用される共通の分母であると偽装することで、自分自身に害を及ぼす可能性があります。それは「かばん語」で、複雑な問題を表現する簡単な方法ですが、この簡潔性が政策にとって悪いガイドになっています。リスクを管理するためには、より多くのレベルでより異なるアクターによる行動が必要ですが、いくつかのデータ駆動の原則が意思決定の手助けとなります。ＩｏＴデバイスの使用によって発生するリスクは、管理し、減少させることができますが、そのためには、研究、規制、インセンティブの組み合わせが必要です。

サイバー空間をより安全にすることを妨害する同じような問題、すなわち、技術的不確実性、限定的な国際協力、改善のためのインセンティブの欠如、安全のための限定的な監督権限、脆弱なオンラインＩＤ、個人データ活用によるインターネットビジネスモデルなどは、ＩｏＴセキュリティの進歩を減速させます。同時に、サイバー空間をより安全にするための同じアプローチは、ＩｏＴデバイスの使用によって発生するリスクを管理し、減少させるために使うことができます。それは、研究、インセンティブ、規制です。ホワイトハウスは、大統領令第１３６３６５号に規定された重要なインフラに対するアプローチを繰り返すことができます。更に、企業が、使用、販売するＩｏＴデバイスに対するセキュリティを改善し、確保するために、担当機関に、企業と協力する任務を付与することもできます。もし、政府、企業、消費者が、インターネットにアプローチするような方法で、ＩｏＴにアプローチすれば、責任、プライバシー、コストに関する現在の規則をＩｏＴに拡大し、そして、既存の法律的枠組みのどこが不十分であるかを識別することによって、新しい法律や規則を制定するか、あるいは裁判所に責任を明確にさせるような「慣習法」のアプローチをとるのかにつながることを意味します。この「拡大」のプロセスは、プライバシー、セキュリティ、ＩＤのようなトピックにとって重要な意味を持っています。なぜなら、現実の世界のために作られた既存の法律や政策の一部は、インターネットにとっては不十分であり、新しい法律、規則、政策の作成を必要とするからです。

どこでいかにしてＩｏＴデバイスを使用するかは、リスクとコストの増大に対し、いかにより良い実績とのバランスをとるかという、ビジネス上の決定です。良い政策はこれらのビジネス上の決定を､簡単にするために役に立ちます｡政策や法律によって企業、消費者は、いかにしてリスクと責任を扱い、どこに投資すべきかを明確にすることができます。

もし、リスク評価のために三つの指標を使うなら、ＩｏＴの意思決定を改善することができます。それは、データの価値、機能の重要性、故障の拡張性です。これにより、政策決定者、監督官、立法者が、ＩｏＴを安全にするため政府の介入が、どこで必要なのか、そして、どこでそのような行動が必要ではないのかを識別することが容易になります。冷蔵庫やエアコンを切ることは迷惑なことです。飛行中にジェットエンジンを切ることは生命にかかわる脅威です。機微な機能を持つＩｏＴデバイスには、高度の審査とセキュリティの努力が必要です。ＩｏＴは、遂行する機能が生命と安全にとって重大であったり、生み出すデータが、本当に機微なものであったり、そして、妨害の効果を拡張することができる場合にリスクを創り出します。これらを行うデバイスは、政府の行動によって高度の水準に維持されなければならなりません。これらを行わないデバイスは、それを修正するために、市場の力や裁判所の行動に委ねることができます。

自律性に関する決定は、ＩｏＴデバイスのセキュリティにとって鍵となる決定要素です｡もし､人間のオペレーターがＩｏＴのオペレーションに介入することができるなら、

リスクは減少させることができます。同時にこれは利益を減少させます。そこで社会は、どこで、どの程度までデバイスの自律性を受け入れるか、そして、どこで人間の介入する能力を維持するのかを決定する必要があります。機能の機密性と、効果の拡張性の指標を使用することにより、どのデバイスが、自律化のために制限や抑制を必要としているのかを識別することができます。

「故障の拡張性」は、リスクを決定するのに役立ちます。悪戯や重罪を超える行動をするためには、ハッカーは、大規模な効果を達成する必要があります。これは、（ありそうにはありませんが）数百、数千ものデバイスを同時にハッキングすること、あるいは、他の多くのデバイスを制御するＩｏＴデバイスを発見することを意味しています。

これらの「コマンド」デバイスは高度の審査とセキュリティ上の注意が必要です。その他のデバイスには必要ありません。国土安全保障省（ＤＨＳ）は、重要なインフラの単一障害点を識別し、そしてＩｏＴにとって「パーフェクトストーム（完全な嵐）」の状態を識別する措置を取らなければなりません。それは、ＩｏＴの故障の組み合わせが（悪意のあるもの、または自然のものであれ）悲劇的な結果を引き起こすようなあり得ない状態をいいます。ホワイトハウスは、重要なインフラに対して２０１３年２月のアプローチを繰り返すことができますし、担当機関に、企業が、使用販売するＩｏＴのセキュリティを改善するために、企業と協力するよう任務を与えることができます。同様に、ＩｏＴに適した軽量の暗号化や認証スキームに関する研究に投資することは、民間セクターがＩｏＴに適したソフトウエア製品を作るための行動を強化します。

ますます増加するイノベーションのプロセスを通じて、ＩｏＴは、時間とともにより安全になりますが、研究、規制、インセンティブ、特に、ＩｏＴデバイスをより安全にする費用対効果の高い方法に対する研究開発費を増加させることによって、このプロセスを加速することができます。インセンティブの中には、訴訟の結果によるものもあります。もし、ＩｏＴデバイスが故障すれば、原告は損害賠償を要求しますし、裁判所は、その責任を明確にします。技術的な規定を回避するよう慎重に作られた規制は、改善を加速化することができるし、輸送、保健、消費財の安全に関する現在の権限は、ＩｏＴをカバーするように更新することができます。

防止可能な事故の頻度やリスクを減少させることは公共の関心事ですが、これには、完全なＩｏＴセキュリティは必要ありません。寓話に基づいた証拠や、仮想の状況に基づいた予防的な行動は、より良いセキュリティのための発明力を減速させ、改善を阻止します。ＩｏＴのイノベーションがどのような道をたどるのか、あるいは消費者が、いかにしてそれを使用しようとしているかは分りません。そのため、実験や新発見する能力の余地を残しておかなければなりません。使用するモノに対する完全なセキュリティはありません。技術が進化するにつれて、イノベーション、規制、市場の力が、リスクを減少させますが、進化した技術であってもリスクは依然として存在します。獲得する利益のほうが何か悪いことが起こるという予想よりはるかに大きいということを、評価

することが必要です。

これは、最初のインターネットが商品化されたときに直面した決定に非常によく似ています。つまり、経済的利益を得るために安全性の低い商品を急速に展開することを選択するのか、より良いセキュリティの実現を待つために展開（またはイノベーション）を遅らせるかという決定です。インターネットの場合、インターネットの利益を享受するためにリスクを容認することが決定でした。これは正しい決定であり、ＩｏＴにも同様な決定をすることが必要です。

ＩｏＴデバイスに対し、セキュリティやプライバシーを要求する権限を与えることがもう一つの選択肢です。これは、行うより言うが易しです。なぜなら、ＩｏＴデバイスがより安全に作られているとしても、それは依然として不安全なネットワークに接続されているからです。ＩｏＴのセキュリティは、サイバーセキュリティと同じ問題に直面しています。ソフトウエアの脆弱性は、誰かがハッキングをしようとして、粘り強く続ければ成功する程度のものです。にもかかわらず、誰もがコンピューターやインターネットを使います。これは、管理者、投資者、消費者のリスクに関する決定を反映しています。ＩｏＴは、ハッキングされるデバイスの数を増大させますが、増大の結果は、まさに機能の重要性、拡張性、データの機密性にかかっています。ＩｏＴリスクを減少させることができる分野の一つは、政府の行動にあります。政府は、国際的なセキュリティに対して独特な責任をもっています。もし、米国が責任ある行動基準を作り、国家間協力を増大させ、悪意のあるサイバー行動を最小限にする共同戦略を策定するために国際的行動をとれば、脅威の環境は作り変えることができます。これは、サイバー空間における組織的なリスクを減少させる最も良い手段です。なぜなら、悪意のある行動によるリスクは、国家あるいは国家が、隠蔽し、保護し、処罰を拒否しているサイバー犯罪者によって作られるからです。ハッカーがどこにいようとも、国家が協力する悪意のあるＩｏＴ行動に対して法の執行や刑事罰を拡大することは、リスクを減少させます。

ＩｏＴデバイスの導入は、ゆるやかで、改善はますます増加します。これは、リスクはＩｏＴデバイスの第一世代のほうがより大きいことを意味します。ＩｏＴがリスクを最小限にする方法で採用されることを保証するためには、極めて短い時間しかないという危惧は間違っており、これから数年のうちに、数十億ものＩｏＴデバイスが出現するという推定は誤った印象を与えています。例えば、米国における自動車の耐用命数は平均１２年です。冷蔵庫は１５年ごとに買い替えられる傾向があります。これは、今から１０年たてば自動車と冷蔵庫の半数以上が依然として「頭の悪い」ままで、リスクの増大にはならないことを意味します。更に、今から１０年後に冷蔵庫を買い替える人は、単に経験やイノベーションという理由で改善されたより安全な「スマート（賢い）」器具を買うことになります。

重要なインフラ、特に大きな資本財には、一般的に長期間の「リフレッシュ」サイクルがあります。このリフレッシュサイクルは、リスクの増加を最小限に抑えます。例え

ば、スマートグリッドのように、導入のペースが改善のペースを上回るようなＩｏＴの急速かつ広範囲にわたる導入には注意が必要です。

## 10. データの保護とプライバシーのリスク管理

ＩｏＴのセキュリティとサイバーセキュリティは、一般に、プライバシーとサイバーセキュリティに関する発想の転換から利益を享受しています。ここ２０年間の努力の多くが､侵入に対するセキュリティネットワークと脆弱性の減少に焦点を当ててきました。あまりにも悲観的すぎるとは思わないが、これらは希望のない仕事です。意思の強い侵入者は、特に十分な資源が与えられている場合には、通常、ネットワークへのアクセスを手に入れることができます。多くの製品が何百万ものコード（符号）に依存しているため、ソフトウエアは非常に複雑になっており、すべてのエラーを回避、発見することは不可能です。サイバーセキュリティに対するアプローチの転換は、ネットワークではなくデータの安全を追求するものであり、機能低下の環境でさえも重要な機能が継続的に作動することを追求するものです。

データの保護とプライバシーには同じような選択肢があります。ＩｏＴデバイスにより作られたデータのセキュリティに対し、すべてに対応可能なアプローチは、奇妙な結果と必要のない障害を創り出します。航空機のエンジンメーカーの事例をとれば、航空機のエンジンは、現在では自動的に整備センターへ状態を報告しています。中には、整備センターの整備士の名前まで含まれるものもあります。個人情報（ＰＩＩ）のために開発されたデータ保護の規則は、ＩｏＴにとっては役に立ちません。単に、ＩｏＴデータにＰＩＩが含まれているという理由で、それが価値のあるものや機微なものであることにはなりません。オンライン契約のために開発されプライバシーの規則は、ＩｏＴの世界では修正が必要です。

ＩｏＴは、国境を越えて移動し蓄積されるデータ量を大きく拡大します。そして、プライバシーにとってもう一つの課題を創り出します。ＩｏＴは、データの局地化という複雑な問題と国境を越えたデータの流れを制限する努力を複雑にするだけですが、（一般的にこれらの規則によくあるように）それらは、グローバル市場にサービスを提供する製造者メーカーに対する障害となります。ほとんどのＩｏＴデータに価値はなく、プライバシーに影響を及ぼすこともありません。ＩｏＴデバイスのデータ使用を制限する規則は、情報の価値を考慮しなければなりません。ドイツの自動車メーカーは、外国の顧客からオンボードモニターを使ってタイヤの空気圧に関するデータを収集し、それを加工して売却するかもしれませんが、プライバシーに対する被害は発生しません。このＩｏＴデータの価値は、たとえ集計されたとしても極めて低いのです。規制と協定にはこれを反映させることが必要で、価値とプライバシーの機密性（デバイスのデータと個人健康データのように）によってＩｏＴデータを分類することも必要です。

データ保護は、公共の政策とビジネスの決定の間に、避けることのできない対立を生

み出します。主要な対立は、機能やデータの価値、あるいは機密性を反映していないセキュリティやプライバシーに対する包括的な解決策を公共の政策に押し付けるという誘惑です。ほとんどのＩｏＴデータに対しては、厳格なプライバシーの保護は必要ありません。ＩｏＴは、保護のための尺度と潜在的な脆弱性だけでなく、データと機能の価値や機密性によって決定される実際のリスクの度合いを反映したセキュリティ手段を必要とします。すべてのデータが同じ価値を持つという議論は時代遅れであり、正確ではありません。

ＩｏＴのデータは、どこに暗号化のような付加的な保護が必要なのか、(暗号化はコストとデバイスの複雑性を増加させるので)、どこでデータが特別な処置を必要としないかを決定するために解析する必要があります。すべてのデータが同じ価値を持つという議論は時代遅れであり、正確ではありません。重要なデータと重要でないデータ（個別又は集計された）を区別することや（生命の安全または潜在的な経済的損失のような）重要性を定義することによって、どのＩｏＴシステムに懸念があるのかを識別することができます。これらの指標を使用すれば、ＩｏＴが安全とプライバシーにとって受け入れることのできないリスクを増大させるのは、ごく限られたケースのみであるということを発見することができます。

## 11. ダイナミックな社会はリスクを容認する

ＩｏＴは、最初のインターネットのために設計されたプライバシー保護とセキュリティの「ミス」を回避する機会を「やり直し」としてアプローチされることがあります。ＩｏＴのセキュリティとプライバシーに関する疑問は、インターネットのセキュリティとプライバシーに関する一般的な議論の延長です。問題は同じです。役に立たない方法を変化させたものはリスクに対する態度です。インターネットは、より楽観的な時代に商業化されました。その時代では、人々は、新しい技術が保有するリスクに対して寛大でした。インターネットのセキュリティは、市場、個々の企業の決定、そして非常に軽い規定に委ねられました。このアプローチが、犯罪がはびこるだけではなく莫大な経済価値を生み出すインターネットを創り出しました。犯罪には数十億のコストがかかりましたが、かわりに数兆もの経済価値を獲得しました。誰もがこのトレードを受け入れるべきです。インターネット時代の初めに、もしセキュリティの要求とプライバシーの制限があったならば、爆発的な成長はあり得ませんでした。

リスクに対する寛容は、安全に対する公共の認識と技術に対する理解の深化と相関しつつ、ダイナミックで時間とともに変化します。サイバーリスクに対する認識は、悪意のあるサイバー事件の数と範囲をよく自覚することによって促進されます。しかし、これらの認識はあまりにも不正確なので、それ自体が、政策に対して役に立たないし、寓話による証拠や仮想的状況の議論によって改善された認識でもありません。人間の発明力と市場の力が、ＩｏＴ技術をどの方向へ導くのか分かりません。経験とイノベーショ

ンによって時間の経過とともにリスクが減少し、新しい技術により安全になることが知られています。もし最初のインターネットが、セキュリティとプライバシーに全く注意を払わなかったなら、現在は、誰も過剰に弁償することを望みません。使用するすべての技術にはリスクがあります。ＩｏＴを恐怖のとりこにしておけば、チャンスを犠牲にすることになります。

著者について

ジェームス・アンドリュー・ルイス氏は、戦略国際問題研究所（ＣＳＩＳ）の上級研究員、戦略技術プログラムの局長です。ＣＳＩＳに所属する前は、国務省で外交官、商務省で上級公務員として勤務しました。また、通常兵器・技術移転及び軍事・情報関連技術の交渉者として、アジアの政治・軍事問題に関する勤務を経験してきました。ルイス氏は、民間・軍事の先進技術に関するワッセナー合意専門家グループの米国代表を経験し、情報保全に関する政府専門家国連グループの２０１０年、２０１３年、２０１５年の報告者でした。

ＣＳＩＳに所属後、ルイス氏は多くの発刊物を著作しています。最近は、オバマ大統領によって賞賛された「第４４代大統領のためのサイバーセキュリティ」などサイバーセキュリティを中心とした仕事をしています。同氏は国際的に有名な専門家で、コメントは頻繁にメディアで取り上げられています。中国現代国際関係研究院と緊密な研究パートナーシップを保有しています。現在の研究は、インターネットの主権、サイバーセキュリティ基準、戦争やイノベーションに関する調査です。ルイス氏はシカゴ大学の博士号（ＰｈＤ）を保有しています。

平成２９年発刊資料

ＢＳＫ第２９－２号『企業が国際共同開発に参加する場合の契約制度上の課題等（その４）（平成２８年度）』
ＢＳＫ第２９－１号『中国のサイバー攻撃の実態（平成２８年度）』
本報告書の中で意見にわたるものは、委託研究先の見解であることをお断りしておきます。

## Ｉｏ Ｔのリスク管理（平成２９年度）

平成２９年８月発行
非売品　　禁無断転載・複製
発　行　：　公益財団法人　防衛基盤整備協会
編　集　：　防衛基盤研究センター刊行物等編集委員会
〒160-0003　東京都新宿区本塩町２１番
電　話　：　０３－３３５８－８７５４　　ＦＡＸ　：　０３－３３５８－８７３５
メール　：　koueki@bsk-z.or.jp
ホームページ　：　https://ssl.bsk-z.or.jp

# 平成27年度情報セキュリティ川柳入選作品

主催　公益財団法人 防衛基盤整備協会

**最優秀賞**

友好が
写真アップで
絶交に

ペンネーム　友情報

**佳作**

そのサイト
白雪姫も
実は魔女

ペンネーム　三郎

**佳作**

「同意する」
規約長すぎ
ついボタン

ペンネーム　楓すず

**佳作**

四季問わず
国境超えて
サギの群れ

ペンネーム　三郎

**佳作**

『重要』の
疑似餌が踊る
詐欺メール

ペンネーム　ばいなりい

**ヤング奨励賞**

詐欺かもよ
そのワンタッチ
考えて

ペンネーム　頭川成葉