情報セキュリティでＩｏＴを実現する
― ＩｏＴのもたらす未来 ―

＜はじめに＞

2021 年 4 月 17 日夜、米国電気自動車大手テスラ※1 のモデル S で走行中の男性 2 人が米テキサス州ヒューストン近郊で木に衝突し死亡した。CNN によると、「運転席には誰も座っていなかったと警察は見ている」という。ロイターによると、「米道路交通安全局（ＮＨＴＳＡ）と米運輸安全委員会（ＮＴＳＢ）はこの衝突事故について調査しており、『車の操作と事故後の火災に焦点を当てる』」としている。さらに、「ＮＨＴＳＡが調査しているテスラ車の事故は今回で 28 件目となった。ＮＨＴＳＡは先月ロイターに、オートパイロットの使用と関連があると考えられるテスラ車の衝突事故について、27 件の特別調査を開始したと明らかにした。このうち 23 件は調査が継続中」という。

2009 年 12 月 8 日午前 5 時 21 分、愛知県西部、三重県北部、岐阜県西部で供給電力の電圧が瞬間的（0.07 秒程度）に低下した。この電力供給トラブルに伴い、キオクシア（東芝四日市工場、三重県四日市市）の主力製品の“ＮＡＮＤフラッシュメモリー”の生産が操業停止となり、翌年 1 月から 2 月にかけてＮＡＮＤフラッシュメモリーの出荷量が大きく落ち込み、約 100 億円前後の減収となった。このように、現代の産業の多くは、国中に張り巡らされた電力ネットワークによって供給される電力に依存している。この中部電力東海地区瞬間電圧低下事故のようなほんの一瞬のトラブルでも、最新鋭工場が停止してしまう事を広く知らしめた。同様の事例として、2016 年の埼玉県新座市の変電所送電ケーブル火災事故で、最大約 58 万 6800 戸が停電し、中央省庁が集まる霞が関まで被害が及び、サーバーがダウンした役所もあったという。

また、以上のような事故ではなく、意図的に起こされた事故もある。すでに、米国のダム管理システムが、イランのハッカーによる攻撃を受けたことが報道されている。また、2015 年 12 月 23 日のウクライナの西部の都市イヴァーノ＝フランキーウシクでの停電では、ウクライナとの間で問題を抱えているロシアのインテリジェンス機関の関与が疑われている。日本経済新聞によると最近も、「米石油パイプライン最大手のコロニアル・パイプラインは 7 日、サイバー攻撃を受けて全ての業務を停止したと発表した」という。今回の事件によって東海岸では、約 5 日間にわたって燃料の補給が絶たれた。

そのような点を踏まえて、サイバー攻撃が物理的な部品を破壊できるかを確かめるために、米国では、アイダホにある ＩＮＬ（Idaho National Laboratory）という研究所によって、2007 年 3 月に「Aurora Generator Test※2」と呼ばれる実験が行われた。27 トンもある巨大なディーゼル発電機を実験用に設置し、停電と通電を繰り返し、発電機を故障させることができるかを確かめようとした。その結果たった数度の停電と通電の繰り返しで、発電機は、大きく振動した後異常な煙を吐き出し動かなくなった。実験のため攻撃は一定のサイクルで行われたが、実際の攻撃ではもっと効果的に短時間で破壊することができると考えられている。

このように、一般報道によって私たちが知り得る情報だけを考慮しても、現代社会はセキュリティ面で極めて脆弱なインフラに依存していることは明白である。

ましてや現代は世界中がインターネットで繋がる時代であり、潜在的な情報セキュリティ上の問題を放置して未来はない。さらに近未来においては、世の中に存在する様々な物体（モノ）に通信機能を持たせ、インターネットへの接続や相互に通信することにより、自動認識や自動制御、遠隔計測や遠隔操作などを行うというＩｏＴ（Internet of Things）の時代が間もなくやってくる。ＩｏＴは近未来のインフラの要となるとされ、農作物や災害危険地区の遠隔監視に始まり、通信網や電力網をはじめとする社会・公共インフラの

常時監視や交通状況の制御、医療の遠隔化やリアルタイム化などが今にも実現されると言われ、この分野は、量子コンピュータやＡＩ（人工知能）と並んで有望視されており、巨額の投資が行われている。

自動車の自動運転や、スマートグリッドの分野でも、ＩｏＴが重要な役割を果たすと目され、世界中で研究開発や実証実験が進められている。しかしながら、これらもＩｏＴが持つ前述の如きリスクを内包する。

以下、ＩｏＴがもたらす世界と、そのリスクについて考察する。

＜Internet of Things＞

様々なネットワークのネットワークである「インターネット」は、人類の生活様式に近年で最も影響を与えたといっても過言ではない。

筆者はインターネットがほぼ完成した 1980 年代の終わりに渡米し、広く普及する直前に開発が目の前で行われていく様を目の当たりにした。最初は全米で使われていたＩＢＭのコンピュータとＭＩＴ（マサチューセッツ工科大学）の地下室でケン・オルセン等によって開発されミニコンピュータのスタンダードであったＤＥＣのコンピュータの間でさえデータを共有させるのは面倒で、再度キーボードで打ち込まなければならなかったものを、互いに理解できるプロトコルを採用することで、互いがつながるようになった。特に、ＭＩＴの同窓会会長を一時期務めたロバート・メランクトン・メトカーフ（Robert Melancton Metcalfe)等によるイーサネットや、ヴィントン・グレイ・サーフ（Vinton Gray Cerf）等によるＴＣＰ/ＩＰプロトコルの標準化を経て、1983 年頃からネットワーク同士がつながるインターネット上でもコンピュータ同士が通信できるようになった。しかしながら当時の時点で、当初暗号技術の本命と考えられた公開鍵方式に脆弱性が発見されており、解読されない暗号技術も完成していなかったため、インターネットはセキュリティに不安を残したままで世界中に普及することとなった。それでもその後ハイパーテキスト転送プロトコル（ＨＴＴＰ、Hypertext Transfer Protocol)やＷＥＢブラウザが導入されると、一般の人々まで広く使うようになった。Windows95 とネットスケープが導入された 1995 年は一般向けインターネット元年とも言われている。さらに 1994 年の筆者等のＡＳＰ（Application Service Provider）の考案に端を発するクラウドコンピューティングが普及し、そのキラーデバイスとしてスマートフォンが登場するとこの流れは決定的となった。今でもセキュリティに関する不安を口にする人は多いが、圧倒的な利便性の前に根本的な解決を待つ人は少なく、インターネットなしではビジネスはおろか生活さえできないという人まで現れ始めている。

人類は歴史上初めて、世界中がネットワークでつながり、リアルタイムで情報伝達/情報交換できる恩恵を受けることとなった。しかしインターネットが人類にもたらしたものは新しい時代の単なる道具というだけではない。新たな時代の思想である。

ネットワークのもつ冗長性やデータのパケット化は一見無駄が多く非効率に思えるが、もともと核攻撃を含む通信網の破壊に備えて開発されており、一部の損傷や故障には十分に耐えられる。パケット化によりネットワークの共同利用が可能になり稼働率を高めることに成功した。その結果、いつでも、必要ならば常時繋げておくことができ、それまでは長距離であれば驚くほど高額だった通信料金を劇的に下げることに貢献した。さらに世界中の通信料金を誰にとっても定額の料金にした。情報の取引に関していえば、世界から距離を消失させ、世界を平等にしたのである。インターネットによって変化した私たちの常識や意識はもはや元には戻らない。それどころか私たちは、この変化が加速することを望んでいる。

これから先インターネットはどのように進化していくのであろうか？

これまでの人類の試行錯誤から多くを学ぶことができる。

攻撃にも故障にも強いネットワークによって、データが送受信されることに啓発されて、リアルタイム性が要求される音声通信でも新たな通信手段が生み出された。また、ネットワークが本質的にすべてを直接結

び付けられ、行政の境や場合によっては国境さえ越えて長距離でも瞬時に情報交換できることを利用して、生産者と消費者を直接繋げるインターネットコマースと呼ばれる新たな市場が生み出された。

通常ネットワークに繋がれるのは通信デバイスであるが、その先に様々なセンサーを繋ぐことでセンサーネットワークを構築し、地球そのものをリアルタイムで測定/監視する試みが行われている。地震などで土砂崩壊などの被災可能性が高い場所に歪計を多数設置して災害を未然に防いだり、農場に温度計や湿度計、風量計、カメラ等を設置して遠隔育成を試みたりしている。最近では繋ぐ先が農産物そのものや野生生物にまで拡がってきている。またその先にコンピュータを繋げば、繋げられたコンピュータ同士が互いに共同作業できることから、ネットワークそのものが巨大な並列コンピュータに進化し得る。すでにグリッドコンピューティングやクラウドコンピューティングなどが実現し始めている。

インターネットは、『Information-Share Platform』として、ポータル、検索、ソーシャルと、主に広告収益モデルとして発達してきたが、近い将来には、第 2 ステージとして、価値の交換が可能な『Value-Share Platform』に進化する。さらにその先において、情報とは全く異なるモノ、例えばエネルギーやモノそのものを情報や価値と共にシェアする究極のプラットフォームに発展していく。

現時点のＩｏＴは、離れた場所の状態を知る「遠隔監視」や離れた場所の状態を変える「遠隔操作」に焦点があてられているが、情報セキュリティの力を得て、究極のプラットフォームに進化すると考えられる。

以下、自動車の自動運転とスマートグリッドを例にして、未来のＩｏＴについて考察する。

＜自動車の自動運転＞

数年前から、米国シアトル近郊のマイクロソフト本社周辺やシリコンバレーのグーグル周辺をドライブしていると、自動運転の実験車両を頻繁に見かけるようになった。両社とも実験車両に最新のカメラ、センサー、そして人工知能を搭載し、実際に運転を行って、人工知能を用いた深層学習※3 を行わせている。グーグルの自動運転では、GPS（全地球測位システム）やレーザーカメラ、レーザースキャナを使い、様々な道路情報（周辺の車両、歩行者、信号、障害物）を収集し、人工知能が総合的に解析し、ハンドル、アクセル、ブレーキなどの運転に必要となる動作の最終決定を行う。この人工知能は、事故予測能力を高めるために、テスト走行中に様々な周辺情報を収集し、それをビッグデータ化して学習する。この学習情報は単体の自動車だけでなく、このシステムを使用するすべての車で共有されるため、学習量は累乗的となり人間の学習をはるかにしのぐ。その結果、今では人間の運転よりも確実に事故率が下がり、近年中に実用化される見込みだという。だが、最近、実験車両ではなく、実車によってグーグルよりもはるかに膨大な量の学習を行っているテスラの自動運転車両が複数回事故を起こしたことで自動運転に対する懸念が多く寄せられるようになった。このテスラに搭載されていたのは先進運転支援システム（ＡＤＡＳ）という自動運転機能で、走行中のハンドルや速度の調整を自動で行うものである。アメリカ運輸省高速道路交通安全局（ＮＨＴＳＡ）の区分※4 では、限定的な環境下もしくは交通状況のみ、システムが加速、操舵、制動を行い、システムが要請したときはドライバーが対応しなければならない状態のレベル 3 であり、専用道路でのオートパイロットが可能で、前の車への衝突を回避し、車線の外に出ていかないようにする。とはいえ、ドライバーは安全確認を継続しなければならないため、ＢMWやメルセデスベンツなど同様の機能を持つ車の場合、ハンドルから手を一定時間以上離せば警告されるようになっているが、テスラにはこのような警告システムは存在しなかった。テスラの場合規則に反してドライバーが完全に手を放して運転していたという事であり、自動運転システム自体に問題があったわけではなかったとも言えるが、自動運転の未来への警鐘となった。特定の状況下のみ、加速、操舵、制動といった操作を全てシステムが行い、その条件が続く限りドライバーが全く関与しないレベル 4 であれば、自身の車両に搭載したセンサー等で収集する情報を解析することによって準自動走行でき

る可能性がある。しかし、ドライバーが全く運転に関与しない完全自動走行（レベル 5）を行うには、周囲の情報を自動車単体が収集して運転するだけでは不十分で、周囲の構造物、通行人、他の自動車の状況などの発信する情報もリアルタイムで集約する必要がある。それにはＩｏＴを用いて周囲と頻繁な通信を行う事で、俯瞰的な三次元地図的交通情報を作成し、その中に自動運転車を位置させることで、より安全に周囲と調和のとれた運転を行え、事故率も激減することになる。これこそが人間のドライバーにはできない、人間以上の安全性が確立できる革新的技術であり、グーグルやテスラなどの最先端企業が狙っている。ところが、現在のＩｏＴ技術では、後述する通り、いくら特殊なＩＣチップを用いてもネットワーク上の個別の「モノ」を正確に遠隔認証することができないため、情報の正当性を保証できず、レベル 5 のネットワークを用いる自動運転は不可能である。今の技術では、センサー情報を解析しながら運転する自律的な自動運転に限られ、十分に安全とはならず、特定の状況下を外れればドライバーの関与が必要であるレベル 4 の実現ができれば良い方であろう。

＜スマートグリッド＞

かつて、電気エネルギーは水力発電所や火力発電所のような発電する場所と、工場や街などの電力消費地が遠く離れており、大発電所から消費地まで一方向の電力網によって供給されていた。電気は蓄えるのが難しかったため、予め電力消費量を予想して、これに合わせた発電計画を立て、できるだけ無駄にならないように発電していた。戦後、原子力発電所が稼働するにつれて、1 日を通して大きく発電量を変えられない特性から、揚水発電所のような事実上の蓄電設備が整備されたが、電力網は相変わらず“一方向供給方式”のままであった。ところが近年、火力や原子力の環境に与える負の影響が知られ始め、また、発電設備を構築・維持するのに必要なエネルギーをその設備が発電するエネルギーで取り戻すというエネルギーペイバックタイム※5 という考え方がエネルギー政策の重要な要素になるにつれて、1 年から 5 年でペイバックする再生可能エネルギーへの切り替えが、ヨーロッパを中心に、次いでアメリカでも望まれるようになった。因みに、火力や原子力は永遠にペイバックしない。他方、エネルギーペイバックタイム的に優れる再生可能エネルギーの中心となる風力発電や太陽光発電では、その性格上あらゆる場所で発電がなされるようになるため、電力網は、一方向送電だけでは不十分となり、双方向送電ができ、かつ、いつでも送電方向が切り替えられることが必要であるから、再生可能エネルギーが普及するにつれて双方向送電の必要性が増してきた。さらに、ＩＣＴ技術（情報通信技術）を用いて、地域全体でエネルギーが余っているところから足りないところへ送電するよう動的に制御することで、時間的にも地理的にも過不足をなくすことができる。これが“スマートグリッド”である。スマートグリッドの整備により、スマートコミュニティと呼ばれる街全体（地域全体）のエネルギーマネジメントや、より小規模にはスマートホームと呼ばれる家の中のエネルギーマネジメントなどが実現すると期待されており、世界中でさまざまな実証実験が行われている。しかし、現在は前述の三重県四日市の中部電力事件やアメリカのオーロラ実験などに代表されるセキュリティに対する懸念から、人間の検針員に代わって電力メーターが電力会社と通信して電力使用量を申告するスマートメーターの各家への設置にとどまっており、本来のスマートグリッドの実現は見えていない。

＜ＩｏＴと情報セキュリティ＞

ＩｏＴでは、専用のチップを様々な物体（モノ）に埋め込み、互いに通信することによって、場合によっては人間さえも介さない、モノのインターネットを実現する。

自動車の自動運転やスマートグリッドのほかにも、自動車の位置情報をリアルタイムに集約して渋滞情報を配信するシステムや、バスや電車のリアルタイムの運行状況を知ることができるシステムなどがある。ま

た、医療分野では、着用型ウェアラブルデバイスによって自分の健康状態を記録・管理し、医師とも共有し、病気の予防と効率的な治療に利用することが考えられており、農業分野でも、水や肥料の量や与えるタイミング、作物の成長の監視などに利用される。

しかし、ＩｏＴのもたらす夢が語られれば語られるほど、一方でセキュリティについての議論が置き去りにされていることについて不安を覚える。特に、自動運転やスマートグリッドについては、人命に関わるだけに、万全の対策を施さなければならない。

ＩｏＴのセキュリティにおける最大の問題点、それは、ＩｏＴにとって最重要と言える認証機能の欠陥である。現在の技術では、いくら専用ＩｏＴチップをモノに埋め込んでも、そのモノを遠隔で正しく認証することができない。つまり、モノとモノの通信が、相手を確認できないままに行われる可能性を排除できないため、情報の発信が正当な権利者によって行われているのか、もしくは正当な権利者になりすました第三者によって行われているのか判別ができないのである。これは、いかに中間者攻撃（ＭＩＴＭＡ、man-in-the-middle-attack）※6を防御するかという、ネットワーク最大の問題が解決できなかったためであり、第三者によるなりすましや通信の乗っ取りの脅威を防ぐことができない。

説明のために分かり易い例をあげると、以前、会社のビルに従業員が入るとき、警備員による本人確認が行われていた。この場合、顔写真が入った社員証を見せることで、社員証が真正であることの確認と、かつ社員証の顔写真と本人の顔が一致することでの本人認証を実現していた。しかし最近は朝の混雑を避けるためか、ＩＣチップの載った社員証を入館改札機にかざすだけで入館できるようになっているところが多い。この場合、社員証の真正性は確認するが、これを所持している人の認証は行わない。その結果、この社員証を拾った人は誰でも入館できることになる。このように社員証自体は偽造不可能なものを作ったとしても、それを所持している人物が果たして正当な所持者であるか否かはシステム上では判断できない。ネットワークにおいても、原理的に本人確認が直接できないのでその所持物によって認証しており、第三者によるなりすましや通信の乗っ取りなどの脅威（ＭＩＴＭＡ）を避けることはできない。ＭＩＴＭＡによる被害を少しでも減らすため、最近ではＩＤとパスワードに加えて、ワンタイムパスワード※7を用いる２要素認証や、さらにバイオメトリクス※8を加えた３要素認証が推奨されており、インターネットバンキングの認証でも２要素認証が当たり前の時代になってきたが、ＭＩＴＭＡに対しては全く無力である。因みに、バイオメトリクスが有効なのは本人が認証者の面前にいるときだけで、バイオメトリクス情報をネットワークを介して送信したとしても認証の完全性は保証されない。

自動車のスマートキーはＩｏＴ応用の一応の成功例と言えるが、最近も、フォルクスワーゲン製の１億台を超える自動車に搭載されているスマートキー※9について脆弱性が発表された※10。これは暗号の脆弱性をついたものである。スマートキーが出始めた頃、固定のＩＤを暗号化したものが鍵に内蔵されており、この暗号化されたＩＤ情報を車載の認証機器に送信して復号化し、正しいＩＤかどうか判定していた。しかし、この暗号化されたＩＤをそのまま盗んで保存し、空のスマートキーに入れれば直ぐに偽造キーが作れるため、盗難は減らなかった。そこで、このＩＤ番号を可変に変更し随分改善されたのだが、スマートキーの容量に制限があり一定数のＩＤを使いまわししたことで、暗号の脆弱性が残ってしまった。それでは暗号の脆弱性を改善すれば盗難は無くなるのだろうか？実は、仮に暗号が完全であったとしても、いとも簡単にＭＩＴＭＡによって多くの車が盗まれているのである。その中でも特に「Amplification Attack(信号増幅攻撃)」が知られており、全ドイツ自動車連盟「ＡＤＡＣ」による実験※11が報告されている。リレーアタックとも呼ばれるが、スマートキーシステムの、外部からの信号に対して内臓のＩＤ情報を応答することによって認証する機能を悪用する。スマートキーをポケットに入れてエンジンをかける場合には、車のスタートボタンを押すことで、車がスマートキーにＩＤ情報を問い合わせ、スマートキーの応答信号を車側の認証装置が真正性

を認定してようやくエンジンがかかる。会社の駐車場に車をとめて、スマートキーをもって会社の会議室で会議を行っている場合を想定すると、スマートキーが車の近くにないので、真正なドライバーがいないと判断されエンジンはかからないはずである。ところが、車からの問い合わせ信号を増幅し、会議室のスマートキーに伝え、今度はスマートキーからの応答信号を増幅して車に伝えることでいとも簡単にエンジンはかかってしまうのである。スマートキー内のＩＤ情報がいかに完璧に暗号化されていようと全く関係はない。最近でもレクサスなどの高級車が立て続けに被害にあっている。さらに最近では、スマートキーに対する極めてシンプルな中間者攻撃（ＭＩＴMA）が報告されている。スマートキーは、①ドアの開錠、②エンジン始動と③ドアの施錠に使用されるが、もし、①で乗車し、②でエンジンを始動し、運転後車を止めて車外に出た後、③の施錠を行う際、犯罪者がスマートキーからの応答信号を妨害電波で妨害すると同時に、応答信号を盗み、ドライバーが施錠されたと勘違いするよう施錠音を鳴らしたなら、ドライバーが去った後、施錠されていない車に乗り込んだ犯罪者はゆうゆうと盗んだ応答信号を使ってエンジンを始動し、持ち去ることができるということである。つまり、この場合の暗号化されたデータは、ビルに入館する際に用いられていた社員証にあたる。暗号化の技術をどれだけ解読不可能に高度化したとても、暗号化された後のデータを中間者に盗まれた場合には、落とした社員証を悪用される場合と同様に、中間攻撃者の悪用を防ぐことはできない。

以上のように、中間者攻撃を排除しない限り、自動運転時の周囲との通信や、スマートグリッドの遠隔監視、遠隔操作は実現不可能である。今のままではテロの危険性を増大させるだけである。

＜中間者攻撃（ＭＩＴMA）を防ぐ＞

ＭＩＴMAの攻撃者は、通常ネットワーク上のどこかに潜んでいると考えられることから、前述の 2 要素または 3 要素認証を行う際に、同じ経路を使って情報を送信するのではなく、例えば、携帯電話網とインターネット網のような複数経路を使って、認証情報を送信することでＭＩＴMAを回避することが行われている。しかしこれは、多少回避できるだけであって、根本的解決にはなっていない。

ＭＩＴMAは、主に①なりすまし攻撃を行った上で、②情報盗聴や③情報改竄を行うのが代表的なものである。②と③については、解読が不可能な現代暗号技術で防ぐことができる。しかし、前述の通り①なりすましは暗号技術だけでは防ぐことができない。ここで本来の認証の目的を再考すると、認証は、人或いはモノが正当な人又はモノであるということを確認するという認証自体を目的とするのではなく、認証が終わった後に行われるアクションが正当な人或いはモノにより行われることを保証することをより本質的な目的とする。言い換えれば、悪意の第三者のなりすましを仮に認証時に許したとしても、その後のアクションを悪意の第三者に許さなければ事実上問題は生じない。以下例を挙げると、

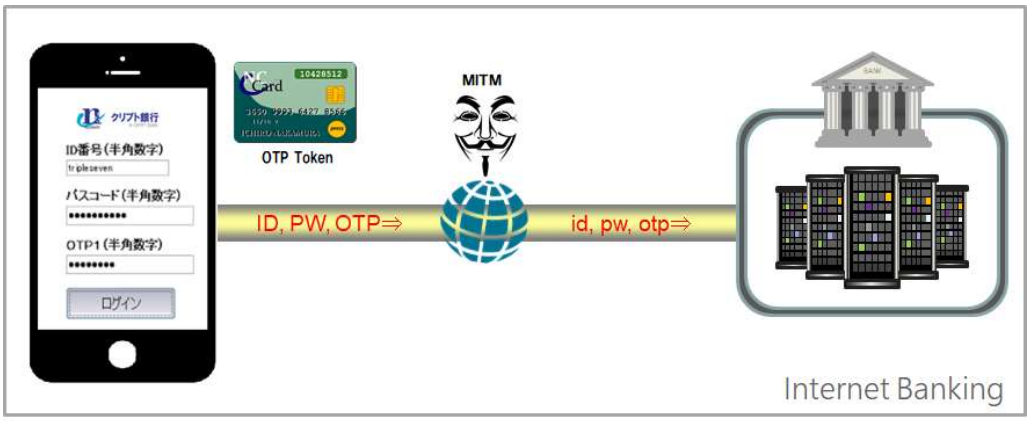
1. インターネットでは、認証した上で、エンド・トゥ・エンドで情報を伝達する。
2. スマートグリッドでは、認証した上で、スイッチングなどの遠隔操作を行う。
3. 自動運転では、認証した上で、周辺情報とシミュレーション情報を更新・交換する。
4. スマートキーの場合は、認証した上で、ドアロックの開閉やエンジン始動を行う。
5. 社員証の場合は、認証した上で、事務所ビルに入館する。

などが考えられる。1 から 3 までは中間攻撃者（ＭＩＴM）が存在することを前提としても、②情報盗聴と③情報改竄を防ぎ、かつ、アクション自体に影響がないようにすれば、問題とはならない。4 と 5 の場合は、②と③を防ぎ、かつ、アクション自体に影響がないようにするだけでなく、これらの認証デバイスを携帯する人と認証デバイスの間の認証を行えばよい。

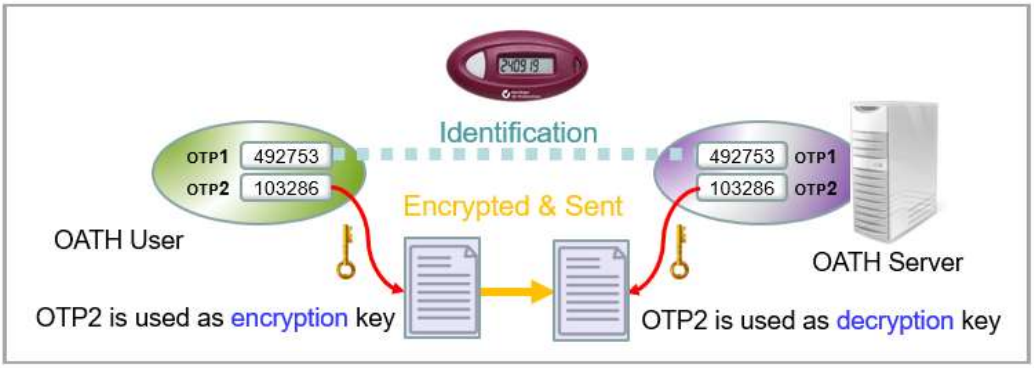
これらの考察から、認証の技術とは別に、仮に認証を破られた場合においても、現代暗号を応用することで

悪意のある第三者が具体的なアクションを行えないようにし、ＭＩＴＭＡを根本的に防げることが分かる。

一例として、スマートフォンのユーザがネットワークを介してインターネットバンキングを行う場合を考えてみると、一般にユーザは、自身に与えられたＩＤと記憶しているパスワードをバンクサーバーに送信してログインを試みるが、これらの情報が中間に潜む攻撃者に取られてしまいそのまま使われれば、なりすましてログインされてしまう。これに対する対策として、ＩＤとパスワードに加えて、2 番目のパスワードや、特殊なワンタイムパスワードトークン（ＯＴＰトークン）を使って毎回変化し 1 回しか使用できないワンタイムパスワード（ＯＴＰ）を生成して、併せて送信しログインする方法や、個人に特定の指紋や顔などのバイオメトリクス情報を送信する方法が実用化されているが、通信の中間で攻撃者に取られてしまえば全く役に立たない。これがインターネットバンキングにおけるＭＩＴＭＡであり、下図のように、悪意のある第三者はなりすましに成功して口座を自由に操作できる。



ところが、既に世界中に広く普及しているこのワンタイムパスワードの使用方法を改良するだけでＭＩＴＭＡを防ぐことができる。ＩＤとパスワードに加えてＯＴＰを送信するところまでは従来と変わらないが、この後もう一度ＯＴＰトークンのボタンを押して新しいＯＴＰを生成し、これを今度は送信しないで暗号鍵の一部として使用して振り込みなどの重要情報を暗号化してバンクサーバーに送信する。バンクサーバーもユーザとは独立にこの新しいＯＴＰを生成することができるので、これを復号鍵の一部として復号化すれば、ユーザの希望通りの振り込みが行われる。この新しいＯＴＰを知り得ない中間攻撃者は情報を盗ることも改竄することもできないので、結果的に中間者攻撃を防御できることが分かる。



＜ＩｏＴの未来＞

情報セキュリティ技術によって真のＩｏＴが実現する未来において、全てがつながる世界がどのようになっていくのか？

真のスマートグリッドが実現すれば、もはや化石エネルギーも原子力エネルギーも必要なくなるだろう。世界中のあらゆる場所で太陽由来のエネルギーを得られ、エネルギー格差は消滅する。エネルギーさえあれば

空気中の水蒸気から飲料水を作ることも、そしてエネルギーと水から農作物を作ることも可能となり、世界の住環境も一変する。地球は歴史上初めて住む地域でハンディを負わない平等な星になる。これを実現するのに、地球よりも寿命が長い太陽から無償で降り注ぐエネルギーのたった数パーセントを利用させてもらうだけでよい。

また自動運転で変わる世界では、運転手という概念が消滅し、また移動するという概念も変更を余儀なくされるであろう。リビングルームが走り出すだけではない。電動化され排気ガスを出さない自動運転車はリビングルームにも入っていく。それどころか、バスルームもシャワールームも必要な時に必要な場所にやってくるかもしれない。未来の海外旅行はベッドに寝そべることから始まるかもしれない。

さらにＳＦ的に考察すれば、地球全体にセンサーのネットワークが張り巡らされ、ネットワークの中に「クラウドインテリジェンス※12」が創造され、すべての気候も、動植物も管理される。人間の行動も思考も管理されることも考えられる。映画「マトリクス※13」の世界も現実味を帯びてくる。

数年前に大流行となった「Pokémon GO」では、スマートフォンの画面上に映し出された目の前の地図や情景に、ポケットモンスターと呼ばれるアニメーションのキャラクターを重ねて映し出す。参加者は実際の公園や街中でこのキャラクターを探すというシンプルなゲームに夢中で周りが見えなくなり、立ち入り禁止区域に侵入したり、交通事故を起こしたりした。このように、現実とコンピュータによって作られる世界とを融合させるＡＲ（拡張現実、Augmented Reality）※14の新たな危険性が指摘されている。また、専用のヘッドマウントディスプレイを装着し、自身がコンピュータグラフィックスの中に入ることが出来るＶＲ（仮想現実、Virtual Reality）※15も、80年代に開発され、世間から待ち望まれていた割にはこれまで長く日の目を見ることがなかったが、機器の値段が劇的に下がり、性能が向上したことで、現実世界のビデオをほぼリアルタイムでモデル化できるようになった。今日では、誰もが自身が現実世界にいるのか仮想現実世界にいるのか分からなくなってしまうほどの没入体験ができる。ＶＲ装置を装着し高層ビルのエレベーターに乗ると、外の景色が急激に変わるのを見て、高速エレベーター内で重力加速度を感じるが、実際は止まった場所でＶＲのビデオを見ているだけだ。自身の脳が過去の経験に基づいた判断をするため、一時的に騙されてしまう。この脳の勘違いがＶＲの本質である。魅力的なＶＲによるコーチがいれば学習効果は何倍にも増すだろう。3か月で英語が話せるようになるかもしれない。人工知能と連動したＶＲの話し相手が、老人ホームで重宝される時代も間もなくやってくるだろう。

ＩｏＴはこれまで、Ｈ２Ｈ（Human to Human、人間と人間がネットワークを介して情報交換をする）、Ｈ２Ｍ（Human to Machine、人がネットワークを通してモノにアクセスする）、Ｍ２Ｍ（Machine to Machine、機械同士がやり取りする）の順で発達してきた。しかしこれらはすべて現実社会におけるＩｏＴであり、仮想社会での役割は想定されてこなかった。ところが最近、ＡＲ（拡張現実）やＶＲ（仮想現実）にも、ＩｏＴが不可欠ということが認識されるようになってきた。今後は、ＶＲ/ＡＲによって表現されるモノから人間への通信や、ＶＲのモノ同士の通信さえ考えられる。ＩｏＴは、Ｒ２Ｒ（Real to Real、現実から現実の情報交換）から、Ｒ２Ｖ（Real to Virtual、現実から仮想の情報交換）、Ｖ２Ｒ（Virtual to Real、仮想から現実の情報交換）、Ｖ２Ｖ（Virtual to Virtual、仮想から仮想の情報交換）を可能にするスマートＩｏＴへと進化し、未来を変え続けていくことだろう。

※1. テスラ

テスラ（英：Tesla, Inc.、NASDAQ：TSLA）は、カリフォルニア州パロアルトに本社を置く、アメリカの電動輸送機器およびクリーンエネルギー関連企業である。テスラ社の現在の製品には、電気自動車、家庭用からグリッドスケールまでのバッテリー電動輸送機器、ソーラーパネル、ソーラールーフタイル、およびその他の関連製品とサービスが含まれる。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/%E3%83%86%E3%82%B9%E3%83%A9_(%E4%BC%9A%E7%A4%BE)、参考：テスラモーターズ HP　https://www.tesla.com/jp/）

※2.　Aurora Generator Test

Idaho National Laboratory ran the Aurora Generator Test in 2007 to demonstrate how a cyber attack could destroy physical components of the electric grid. The experiment used a computer program to rapidly open and close a diesel generator's circuit breakers out of phase from the rest of the grid and cause it to explode.

（出典：Wikipedia　https://en.wikipedia.org/wiki/Aurora_Generator_Test）

※3.　深層学習（ディープラーニング）

脳の仕組みを模した「ディープ・ニューラル・ネットワーク」を使用する機械学習であり「深層学習」とも呼ぶ。ディープラーニングは米グーグルや米フェイスブック、米ヤフーなどが画像認識や音声認識、自然言語処理などの分野で使用しており、認識精度を大きく伸ばしている。

（出典：IT PRO　http://itpro.nikkeibp.co.jp/atcl/column/14/494329/091800020/）

※4.　アメリカ運輸省高速道路交通安全局（ＮＨＴＳＡ）の区分

日本政府や米国運輸省道路交通安全局（NHTSA）では自動化のレベルを以下のように定義している。

レベル０：ドライバーが常にすべての主制御系統（加速、操舵、制動）の操作を行う。

レベル１（運転支援）：加速、操舵、制動のいずれか単一をシステムが支援的に行う状態。

レベル２（部分自動運転）：システムがドライビング環境を観測しながら、加速、操舵、制動のうち同時に複数の操作をシステムが行う状態。

レベル３（条件付自動運転）：限定的な環境下若しくは交通状況のみ、システムが加速、操舵、制動を行い、システムが要請したときはドライバーが対応しなければならない状態。

レベル４（高度自動運転）：特定の状況下のみ、加速、操舵、制動といった操作を全てシステムが行い、その条件が続く限りドライバーが全く関与しない状態。

レベル５（完全自動運転）：無人運転。考え得る全ての状況下及び、極限環境での運転をシステムに任せる状態。ドライバーの乗車も、ドライバーの操作のオーバーライドも必要ない。安全に関わる運転操作と周辺監視をすべてシステムに委ねる。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/自動運転車）

※5.　エネルギーペイバックタイム

エネルギー（電力や熱）を生産（もしくは節減）する設備の性能を表す指標の一種である。特定のエネルギー設備に対して直接あるいは間接的に投入したのと同量のエネルギーの消費を、その設備からのエネルギーの生産によって回避できるまでの運転期間を言う。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/エネルギーペイバックタイム）

※6.　中間者攻撃（ＭＩＴＭＡ、man-in-the-middle-attack）

攻撃者が犠牲者と独立した通信経路を確立し、犠牲者間のメッセージを中継し、実際には全ての会話が攻撃者によって制御されているときに、犠牲者にはプライベートな接続で直接対話していると思わせる。攻撃者は２人の犠牲者の間で交わされている全てのメッセージを横取りし、間に別のメッセージを差し挟む。これは多くの状況で容易なものである。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/中間者攻撃）

※7.　ワンタイムパスワード

一度しか使えないパスワード（使い捨てパスワード）のこと。パスワードを毎回異なるものにして，意味のない文字列を使う仕組みを実装したもの。

（出典：IT PRO　http://itpro.nikkeibp.co.jp/article/COLUMN/20060414/235357/?rt=nocn）

※8.　バイオメトリクス

生体認証（せいたいにんしょう）はバイオメトリック（biometric）認証あるいはバイオメトリクス(biometrics)認証とも呼ばれ、人

間の身体的特徴（生体器官）や行動的特徴（癖）の情報を用いて行う個人認証の技術（プロセス）である。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/生体認証/）

※9. スマートキー

A smart key is a key with digital or information features that can facilitate more functionality than just unlocking a physical or digital lock system.

（出典：Techopedia　https://www.techopedia.com/definition/20080/smart-key）

※10. フォルクスワーゲン製のスマートキーの脆弱性

A new wireless hack can unlock 100 million Volkswagens.

（出典：WIRED　https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/）

※11. 全ドイツ自動車連盟「ＡＤＡＣ」による実験

スマートキーをハックして遠隔チームプレイで手際よく高級車を盗み出す驚愕の手口が明らかに。

（出典：Gigazine　http://gigazine.net/news/20160324-car-smartkey-amplifier-attack/）

※12. クラウドインテリジェンス

人間の知恵である人知と人工知能が作り出す人工知をネットワーク上で統合する技術及び統合された知能。

（出典：https://www.nti.ne.jp/product-service）

※13. マトリックス

1999 年にアメリカで製作された。原題は「The Matrix」。配給はワーナー・ブラザース。キアヌ・リーブス主演で、仮想現実空間を舞台に人類とコンピュータの戦いを描いた SF アクション。人類が現実だと思っている世界が実はコンピュータにより作り出された「マトリックス」と呼ばれる仮想世界であり、本当の現実世界でネオをはじめとした人間たちはコンピュータに支配され、眠らされているという。主人公はコンピュータが支配する世界から人類を救うため戦いに乗り出す。

（出典：https://eiga.com/movie/49688/）

※14. ＡＲ（Augmented Reality）

拡張現実（英: Augmented Reality、AR）とは、人が知覚する現実環境をコンピュータにより拡張する技術、およびコンピュータにより拡張された現実環境そのものを指す。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/拡張現実）

※15. ＶＲ（Virtual Reality）

バーチャルリアリティ（英: Virtual Reality）とは、実際の形はしていないか形は異なるかも知れないが、機能としての本質は同じであるような環境を、ユーザの五感を含む感覚を刺激することにより理工学的に作り出す技術およびその体系。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/バーチャルリアリティ）