ＩｏＴの実現にセキュリティの確立を
Future Ｉｏ Ｔ with ＶＲ/ＡＲ

＜はじめに＞

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、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、100 億円程前後の減収となった。

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。この四日市瞬時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。先日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。

米国では、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、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※1」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。そして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たと考えられている。

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おり、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。

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が分かる。

すでに世界中がインターネットで繋がり、今では、世の中に存在する様々な物体（モノ）に通信機能を持たせ、インターネットに接続したり相互に通信することにより、自動認識や自動制御、遠隔計測などを行うというＩｏＴ（Internet of Things）の時代が喧伝されている。ＩｏＴは近未来のインフラの要ともなり、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、ブロックチェーンやＡＩ（人工知能）に並んで有望視されており、巨額の投資も行われようとしている。

同様に、自動車の自動運転や、スマートグリッドの分野でも、ＩｏＴが大きな変革をもたらすと目され大規模な投資を呼び込んでいる。しかしながらこれらもＩｏＴが持つ上述の如きリスクをはらむ。以下これらを例に挙げ、ＩｏＴがもたらす世界と、そのリスクについて考察する。

＜自動車の自動運転＞

近年、米国シアトル近郊のマイクロソフト※2本社周辺やシリコンバレーのグーグル※3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※4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、テスト走行中にさまざま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ので、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社※5の自動運転車両が事故を起こしたことが話題になり自動運転に対する懸念が多く寄せられた。このテスラに搭載されていたのは高度運転支援システム（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※6では、加速・操舵・制動のうち複数の操作をシステムが行うレベル２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。とは言え、ドライバーは安全確認を継続しなければならないので、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ないようになっているが、テスラはこれを許していた。今回はドライバーが完全に手を放して運転していたという事なので、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。加速・操舵・制動を全てシステムが行い、システムが要請したときはドライバーが対応するレベル３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４）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、その中の自動運転車とすることで、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、グーグルなどの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」を認証することができないので、情報の正当性を保証し得ず、レベル４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、ドライバーの関与が必要であるレベル３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こ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※7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。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から、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になってきた。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、現在は上記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のもたらす夢について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、万全の対策を行わなければならない。

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そのものがもたらす欠陥ともいえるものである。いくら専用ＩｏＴチップをモノに埋め込んでも、そのモノを認証することが必ずしもできない。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、はたまた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）※8 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、第三者によるなりすましや通信の乗っ取りの脅威は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、社員証が真正であり、かつ社員証の顔写真と本人の顔が一致することで認証していた。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※9を用いる2要素認証や、さらにバイオメトリクス※10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※11について脆弱性が発表された※12。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ので、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※13が報告されている。スマートキーシステムでは、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。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。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、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、生成された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おり、多少の効果はあるが、根本的解決にはなっていない。
ＭＩＴＭＡは、主に①情報盗聴、②情報改竄、③なりすましなどの攻撃が代表的なものだが、完全な暗号通信を行う事で①および②は防ぐことができる。しかし、上述の通り、③は暗号通信では防ぐことができない。
ここで再度、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、①情報盗聴と②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、①と②を防ぎ、かつ、アクション自体に影響がないようにしたとしても、さらに、これらの認証デバイスを携帯する人の認証が面前で必要となる。
このような点を考慮すると、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するための技術というのも別途考慮する必要があり、真のＩｏＴ（スマートＩｏＴ）のためには、完全な暗号技術が必要で、特に暗号鍵の配送問題を内包しない技術で実装しなければならない。

＜ＩｏＴの未来＞
今春の発売以来大流行となった「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と、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ので、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、近未来に不可欠の技術となるとなるであろう。
ＡＲやＶＲで作られたオブジェクトやコーチの著作権を守るのもスマートＩｏＴである。大リーグのＩＣＨＩＲＯや、リーガエスパニョーラのメッシの仮想分身の著作権はスマートＩｏＴで保護され、違法コピー/使用は排除される。仮想世界でのシミュレーションも、仮想分身を使ったビジネスにおける課金もスマートＩｏＴによって行われるようになる。スマートＩｏＴは現実世界と仮想世界をシームレスに繋ぐ鍵となるであろう。

※1. 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)

※2. マイクロソフト

マイクロソフト（英：Microsoft Corporation）は、アメリカ合衆国ワシントン州に本社を置く、ソフトウェアを開発・販売する会社である。1975 年 4 月 4 日にビル・ゲイツとポール・アレンらによって設立された。

(出典:Wikipedia https://ja.wikipedia.org/wiki/マイクロソフト、参考:マイクロソフト HP https://www.microsoft.com/ja-jp/)

※3. グーグル

Google Inc.（グーグル）は、検索エンジン、クラウドコンピューティング、ソフトウェア、オンライン広告といったインターネット関連のサービスと製品を提供するアメリカ合衆国の多国籍企業である。収益の多くをアドワーズ（AdWords）と呼ばれるオンライン広告から得ている。

(出典：Wikipedia https://ja.wikipedia.org/wiki/Google/)

※4. 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/)

※5. テスラモーターズ

テスラモーターズ（英: Tesla Motors, Inc.、NASDAQ: TSLA）は、アメリカ合衆国のシリコンバレーを拠点に、バッテリー式電気自動車と電気自動車関連商品を開発・製造・販売している自動車会社である[1]。本社所在地はカリフォルニア州パロアルト。

(出典：Wikipedia https://ja.wikipedia.org/wiki/テスラモーターズ、参考：テスラモーターズ HP https://www.tesla.com/jp/)

※6. 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：加速・操舵・制動のいずれかをシステムが行う状態。

レベル２：加速・操舵・制動のうち複数の操作をシステムが行う状態。

レベル３：加速・操舵・制動を全てシステムが行い、システムが要請したときはドライバーが対応する状態。

レベル４：完全自動運転。加速・操舵・制動を全てドライバー以外が行い、ドライバーが全く関与しない状態。

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

※7. 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）

※8. 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）

※9. 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）

※10. 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/）

※11. 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）

※12. 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/）

※13. 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/）

※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）