未解決サイバーフィジカルセキュリティ課題とその解決に向けて

松本　勉

今日のタイトルは「未解決サイバーフィジカルセキュリティ課題とその解決に向けて」ですが、証券業の皆様にとって、コンピューターネットワークを通じた日々のサービス・業務に直結する部分はもうよく御存じだと思います。したがって、そこからもう少しはみ出た部分、いわゆる証券の対象となっているビジネスのアクティビティの面で、セキュリティに関してどんなことが起きてくるのか、少し先の話も含めつつ見てみたいと思っております。よろしくお願いいたします。

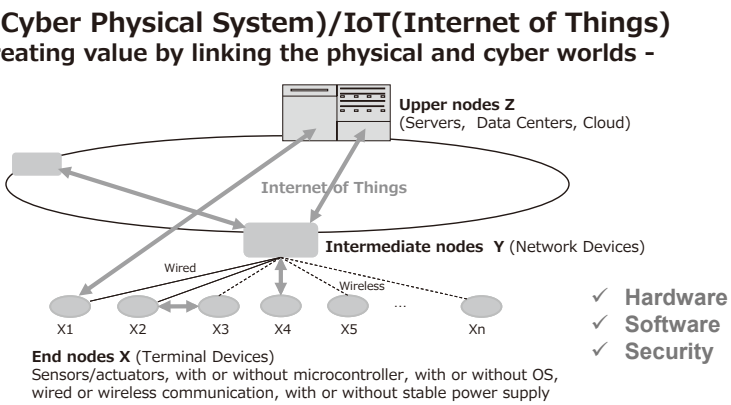
講演の概要です。

イントロダクションとして、このところ非常に浸透してきたCPS（Cyber Physical System）／IoT（Internet of Things）はセキュリティとどういう関係があるのか、お話ししたいと思います。

次に、その中でも特に新しい部分として、計測セキュリティと制御セキュリティ、すなわち、自動車やロボットなど、モノを動かすときにかかわってくるセキュリティの問題について御説明いたします。

そして、少しマニアックにみえるかもしれませ

図表１



Cyber Physical Systems or IoT implicate infrastructures that create new value by connecting many devices with communication networks. Their constructions are rapidly progressing in anticipation of their great potential.

んが、それらの問題を解決するためにさらなる展開が期待される重要な技術がたくさんありますので、その中から幾つか御紹介したいと思います。

最後に、昨今、サプライチェーンのセキュリティやインテグリティが非常に重要となっておりますが、それをさらに極めていくにはどうしたらよいかということで、最近、国際標準規格として設定された人工物メトリクスというエマージングな技術について、さわりをお話しできればと思います。

一、CPS／IoTとセキュリティ

この図の横長の楕円の部分は、いわゆるインターネットです（図表1）。ルーターなど通信のための機器があり、それらが複雑な形でネット

ワークを構成しています。その中には、データセンター、サーバー、クラウドがあり、皆様のお仕事の関係でもそういうものが必ずどこかにあるはずです。このようなインターネットのネットワークはボトムアップで発展してきたわけですが、そこのセキュリティが問題だという話が日々報道されています。

ただ、セキュリティといっても概念は広く、大きく分けて三つあります。

一つ目はコンフィデンシャリティ（守秘性・機密性）で、見ることに関するセキュリティです。本来は特定の人しか見ることができない情報を権限がない人が見てしまう。例えば情報漏洩ということで、サーバーにある貴重な情報が勝手に引き出されるといった問題があります。

二つ目はインテグリティ（一貫性・完全性）で、書くことに関するセキュリティです。情報を変更するにはやはり権限が必要ですが、権限のない人が能動的に書きかえてしまう。先ほどは見るだけでしたが、書きかえるというのはアクティブな攻撃です。

ちなみに、セキュリティの世界では「完全性」という言葉が使われていますが、「完全性」に対応する英語には「コンプリートネス」もあり、異なる意味になりますので、誤解のないように「インテグリティ」という言葉を積極的に使いたいと思います。

三つ目はアベイラビリティ（可用性）で、使うことに関するセキュリティです。昨今、ネットワークがダウンしたら仕事ができないという状況が多々あります。瞬断でもいろいろと問題が起こるので、何日も復旧しないとなると大問題です。

これら三つは誰もが認めるセキュリティの項目ですが、今日の主題である「サイバーフィジカル

セキュリティ」の「フィジカル」が入ってこなくても既に我々が経験していることであり、さまざまな対策もとられてきています。装置的、システム的、あるいはプロセスとして確立されているだけでなく、日々の運用において、不正をいかに早く検知し、対処するかというオペレーショナルな機能も非常に必要とされていることは、皆さんよく御存じのとおりです。

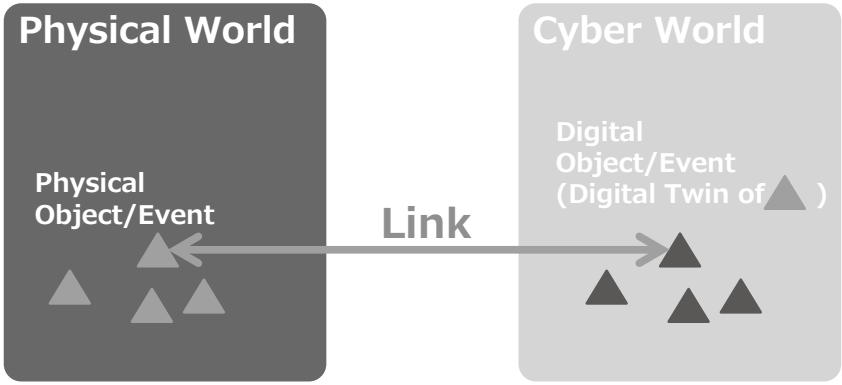
「End nodes」と書いている上の小さな横長の楕円は末端の機器です。ここは無線や有線でつながっており、現実の我々の三次元空間、時間を入れれば四次元空間の世界に作用を及ぼす部分です。上のほうはいわばサイバーワールドで、データが飛び交っているだけです。ただし、コンピューターやネットワークは物体ですので、実態としてはモノの上に成り立っており、そこが攻撃されていろいろな被害が出ないようにしようということですが、そもそもサイバーの世界をつくったからこそ、今のデジタル化の礎があるということにもなるわけです。

末端の機器にはさまざまなものがあります。我々が使っているスマートフォンをはじめ、この部屋にある火災報知器、マイク、プロジェクターなど、全てにコンピューターが入っており、それらがどんどんつながろうとしています。現在でも、例えばBluetoothは当たり前のものになってきていますが、いろんなものがもっと密につながってくる可能性があります。特に、医療機器や自動車といった人命にかかわるものにネットワークが拡張しています。

特徴としては、ネットワークやサーバーの機器に比べて、ハードウェアのリソース、すなわち使える装置の量自体が多くない。安くないと使えない。数はたくさんありますが、一つ一つが小さい

図表２

Cyber and Physical Worlds



ので、機能が限定されていたり、コンピューターの計算能力が低かったり、記憶容量が少ない。あるいは、電池駆動でパワーが弱く、太陽光発電などのエナジーハーベスティング（環境発電）で電源がふんだんにとれるとは限らないケースもあります。

これらのものはハードウェアの上にソフトウェアが載って機能しますが、ネットワークにかかわるエンティティがどんどん増えていく中においては、秩序をもたらしていかなければいけません。そのため、全体としてのセキュリティをどう保っていったらよいのか、こういう頭の痛い問題があるわけです。

今申し上げたことを大胆に抽象化してみたのがこの絵です（図表２）。先ほどの図の下の部分が「フィジカルワールド」、上の部分が「サイバーワールド」です。

フィジカルワールドとサイバーワールドを対応させようということで、人間や動物、建物や機器などあらゆるモノやコト（事象）をデータで再現することを「デジタルツイン」と言います。逆から見たら、「フィジカルツイン」ということになります。ただし、ツイン（双子）といっても、現実の世の中は非常に複雑ですので、等価のものを一対一で表現するのはほぼ無理です。したがって、重要な項目についてデジタルツインになるものを持ってきて、サイバーワールドでいろいろシミュレーションしてみる、つまり、世の中のある局面をサイバーワールドの中で再現してみると、次にどう動くか、どのような状況が生じるかということが予測できるかもしれないということです。

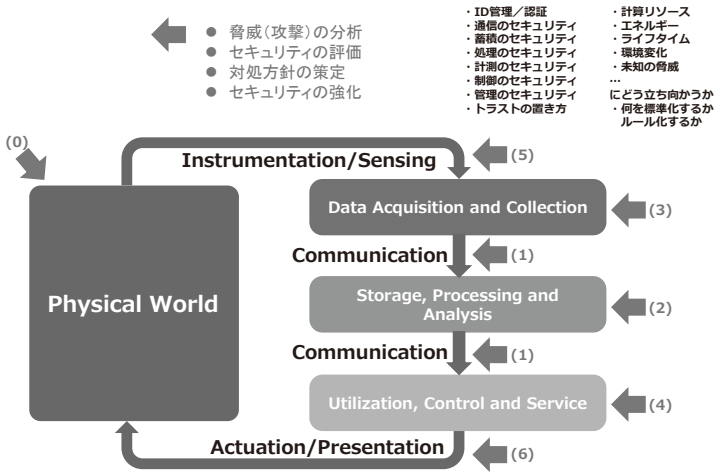
例えば工場で使っている機械です。使用を重ねると劣化し、いつかどこかで使えなくなります。しかし、その機械の状態を常時センサで観察し、あとどれくらいで使えなくなりそうかということが事前にわかれば、計画的に交換でき、製造ラインを止めなくて済むなど、いろいろなメリットがあります。こういったことがインフラのメンテナンスでも徐々に始まってきています。そのほかにも、想像力を豊かにしていただければ、このモデルで何でもできそうだということになります。

そこでセキュリティが出てくるわけですが、サイバーワールドを分解してみたのがこの絵です（図表3）。

同じく機械の例で言えば、まず、フィジカルワールドにある機械の状態を計測器で調べ、状況を把握します。そして、獲得・集積したデータをＡＩなどを使って処理・解析し、交換の時期を予測するなど、もろもろのサービスにつなげていきます。そういう計画が立つと、実際そのとおりフィジカルワールドに作用させるということで、

図表３

サイバーフィジカルセキュリティの課題



モノを動かしたりプレゼンテーションしたりといったことになるわけです。箱の間に「Communication」と書いてあるのは、一カ所でそういうことが行われるとは限らないからで、ネットワークを通じて通信がなされるという形になります。

では、サイバーフィジカルセキュリティという文脈において何を考えればいいのかということになるわけですが、矢印は「脅威」、すなわち起きては困ることをあらわしています。その中には自然災害なども含まれますが、誰かによって意図的に攻撃が行われることを考えておかなければいけないので、ここで言う脅威は「攻撃」とほぼ同義と考えていただいて構いません。

まず、どういう脅威（攻撃）があるのか認識する必要があります。次に、それを分析し、今のシステムでどれくらい耐えられるのか、セキュリティを評価します。もしも十分でない場合、技術

的に対処できないものについては、管理の方法など別のルールによってその脅威をかわせるようにするというやり方もありますし、技術的により優れたものが既にあればそれを適用する、なければ開発してから適用する、そういった対処方針を策定します。そして、その方針に従って実際にセキュリティを強化していくという流れになります。

では、どこでこの矢印（脅威）が関係してくるのかということですが、番号をつけてあらわしました。若い番号のものほど、昔からあることを示しています。

まず、(0)のフィジカルワールドについては、モノを壊す、線を切る、詐欺行為を働く、人をあやめるなど、さまざまなものがあり、これもセキュリティの項目と見ることができます。

サイバー系の脅威（攻撃）として最初に出てきたのが(1)のコミュニケーション（通信）の部分で、盗聴やなりすましです。このような脅威に対しては、暗号技術をはじめさまざまな技術が適用されています。先端的なところはどんどん高度化しつつありますが、最低限どうすればいいのかという一定のレベルはわかってきているものです。

続いて、(2)の処理・解析の部分です。最近、ＡＩにおかしなデータを与えてよからぬ帰結を導き出すといったことが大問題になっており、これからますますフォーカスされていくのではないかと思いますが、処理のセキュリティは比較的早く認識され、研究も進んできているところです。

さらに、(3)のデータの獲得・集積、(4)の活用・コントロール・サービスというところが出てきまして、最後に残ったのが、(5)の現実世界のデータを読み取る、(6)の計画を立てたとおりにモノを動かすという部分に対する攻撃です。このあたり

は、昔から概念としてはあったもののあまり気づかれずにいましたが、最近いよいよ問題になってきたものです。

その上で、右上に記したようなさまざまな課題があります。

まず、モノやヒトのほか、ソフトウェア、あるいはアバターといったものが、どれなのか、誰なのかということを特定できないといけません。匿名性を保つことも含めてＩＤの管理は非常に重要になってきており、そのＩＤどおりのモノなのか、ヒトなのかを確認する認証の問題があります。また、通信、蓄積、処理、計測、制御のセキュリティがあって、さらに全体を管理するためのセキュリティがありますが、そのときに大事なのがトラストの置き方です。トラストとは、技術的な部分での対策をする上での前提をどうするか、つまり、誰も信用できないとしてしまうと何もできないということが起こり得るので、「ここは大丈夫」「ここはそうとは限らない」、そういう整理をして物事を考えるということを意味します。

さらに、先ほども少し申し上げた計算リソースや得られるエネルギーのほか、実世界に埋め込まれたコンピューターはライフタイムが非常に長いので、自然環境の変化だけでなく技術環境の変化も考えなければいけません。日進月歩で技術の進化が進み、攻撃者が使い得る技術もどんどん新しくなってきているからです。そして、現在はまだ顕在化していない、あるいは潜在的にあるともわかっていないものの、将来出てくるかもしれない脅威があり得ます。これを完璧に把握することは非常に困難ですが、いわゆる「想定外でした」ということをなくすのが究極の目標です。

このような制約のもと、セキュリティ対策に立

ち向かっていく必要があるわけですが、いろんなステークホルダーがいますので、標準化しないと使えなくなりますし、ルール化しないと秩序が保てません。どうやってそれを進めていくのかということがさまざまな部分で出てきますので、非常に大変な話だということをわかっていただければと思います。

今の話を整理すると、サイバーフィジカルセキュリティにかかわる脅威は次の三つです。

一つ目は、フィジカルワールドの脅威です。これは先ほどの(0)の部分です。物理的な機器やネットワークの上に成り立っているのがサイバーワールドですから、当然サイバーワールドのほうも麻痺します。例えば、どこかのデータセンターが入っているビルが地震で倒れたり、爆破されたりしたら、そこがかかわっているサイバーワールドの一部は大きな影響を受ける可能性があります。

二つ目は、サイバーワールドの脅威です。この影響はフィジカルワールドにも及びます。昨今、ニュースに出てくるもののほとんどがこれです。

そして三つ目が、フィジカルワールドとサイバーワールドの関連づけを揺るがす脅威です。先ほど対応関係があると申し上げましたが、その対応関係が楽観的に捉えられているケースが多く、そこを曖昧にするような攻撃が出てきています。これはさまざまな局面において多様な形であらわれてきますので、そこのところを深く考えていただけると、私が今日ここに来てお話しした意味があるのではないかと思います。

今申し上げたことを総合して、「セキュリティ保証（Security Assurance）」という考え方があります。

セキュリティは目に見えないので、どういうものかわかりにくいのですが、何らかのアプリケー

ションや応用分野に着目すれば、「そこのセキュリティはこうあるべきだ」というのは、関係者のコンセンサスを得ることによってつくり上げられるはずです。したがって、ある種の物差しをつくらなければいけないということです。

資料では一直線の物差しになっていますが、必ずしも一次元である必要はありません。極論すれば、どのくらい強いかということをなるべく簡単にあらわしたいわけです。例えば、人間の能力を評価するのは非常に難しいですが、ある組織の中で人事の考課表をつくる場合、無理やり一直線に並べざるを得ないということがあります。そういうイメージで考えていただけるといいのではないかと思います。

そして、どうやってセキュリティの強さをはかればよいかがわかったならば、「このアプリケーションにおいては、これ以上になってほしい」という要求水準を関係者がよく検討し、納得する。場合によっては、時間とともにその水準を上げていかなければいけないということもあります。

例えば、皆さんもよくお使いになっているＩＣカードがあります。ＩＣカードのチップのセキュリティについては、非公開の組織が、論文やネットワークで開示されている公開情報及びアンダーグラウンドの情報も全て集め、みずからが攻撃者の役割をしてあら探しをするということを常時行い、その中で、「現時点では、このくらいのセキュリティでないとまずい」というある種の基準をつくっています。一〇年くらい前まではかなり危ないものもありましたが、最近のＩＣカードのチップは、そう簡単には破られないものになっているはずです。それでもなお、攻撃者のレベルをウオッチし、「彼らはまだそこまで追いついてこないだろう」というような形で余裕を見ながら、

新たな基準を定めていくということをしています。そういう業界では年に六回くらいミーティングを開いており、かなり本気度が高いです。もしも破られたら、金銭的及び人的、社会的に甚大な被害が生じ得るので、一生懸命やっているわけです。

しかし、こういう体制すらないところもたくさんあります。世の中はネットワークによってつながっていく傾向がどんどん加速していますので、このようなセキュリティ保証の枠組みをきちんと確立していかなければいけない分野が増えてくると考えられます。

話が途中になりましたが、基準ができたら、それを上回るような技術を誰かがつくって提供し、適用していかなければいけません。ここは競争によって行うと、よい技術が安くつくれるだろうと思います。

ただし、その技術が要求水準をきちんと満たしていることをどのようにして利用者に信じてもらうか、ここが大問題です。エビデンスを伴って自己宣言する、すなわち、「我々の技術が基準を満たしていることはこうすれば確認できます」と客観的に言うことができればよいのですが、そのためには、それを評価する人に、例えば、ソフトウェアのソースコードやハードウェアの設計書、あるいは現物を渡してチェックしてもらう必要があり、情報が漏れるリスクも高いです。したがって、信用できる第三者、オーソリティを設け、そこには情報を伝えるが一切漏れないという体系にして第三者認証する、こういうことが重要な機器やシステム、サービスについては行われています。

この評価・認証の枠組みは、セキュリティに限らずどんな分野においても成り立つ話ですが、特

にセキュリティでは、目に見えないところを見える化するというところが重要になってきます。

二、計測セキュリティと制御セキュリティ

次に、「計測セキュリティと制御セキュリティ」についてお話しします。

フィジカルワールドとサイバーワールドの対応関係を曖昧にする脅威にはどのようなものがあるかという話です。

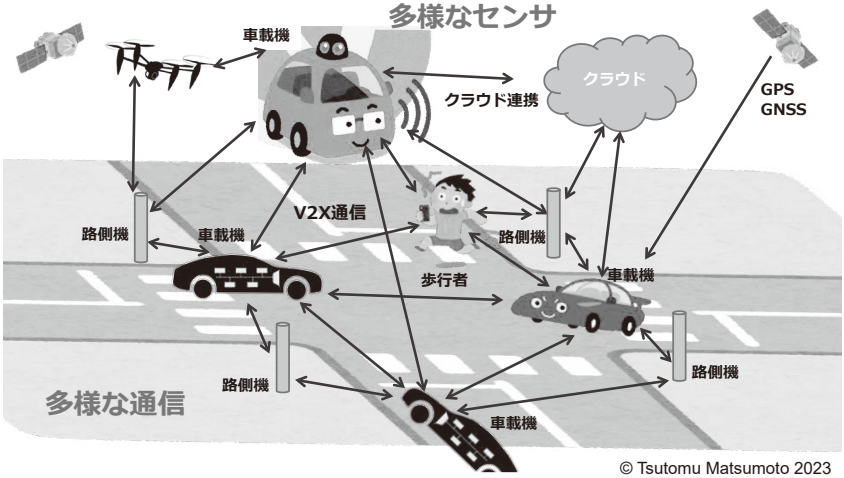
例えばスマートフォンや自動車、冷蔵庫などは、コンピューターやコントローラーが入力に対して何段階かの基本的な処理を行い、結果を出力します。そのときに、その処理をどうやって定めているのかとか、状況に応じてパラメーターを変更するといったことがあるので、メンテナンスをしなければいけません。ですから、大抵のものはプログラムやデータを更新する機能が備わっているのが普通です。

そうしますと、漏洩（コンフィデンシャリティにかかわる脅威）、機能改変（インテグリティにかかわる脅威）、不能化（アベイラビリティにかかわる脅威）といったことが起こるわけです。特にプログラムのところをいじられてしまうのは非常に怖いことです。

例えば、最近の自動車には多くのコンピューターが搭載されており、高級車では一〇〇台以上のコンピューターが搭載されています。その代表的なものが電子制御ユニット（ＥＣＵ）と呼ばれるもので、センサやその他のものとつながって車載ネットワーク（In-Vehicle Network）を構成しています。

また、最近の自動車は外部との通信も普通に行

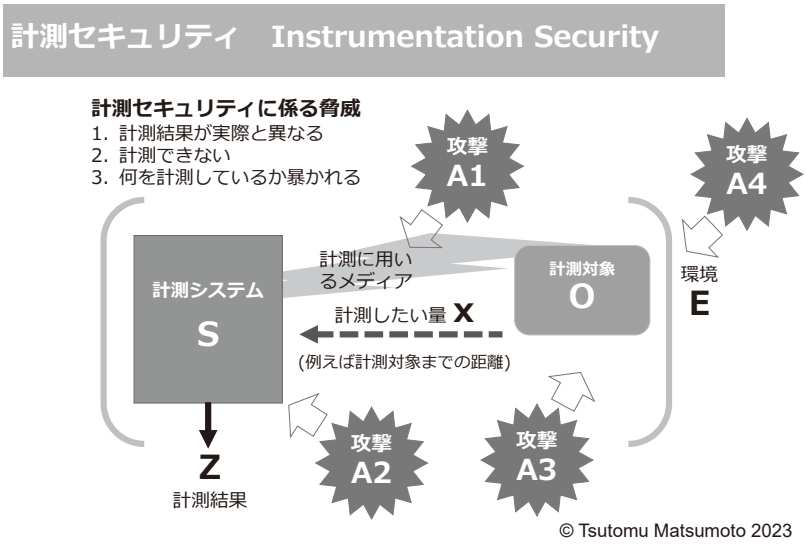
図表４



われるようになっており、この傾向はますます進んでいくだろうと思います。この絵のように、信号機などに設置されている路側機、車同士、歩行者が持っている端末、ドローン、ＧＰＳやＧＮＳＳなどの衛星測位システム、４Ｇや５Ｇを使ったクラウドとの連携など、さまざまなものと通信しています（図表４）。車についているセンサだけでは、自分の周辺の情報をとるのに限界があり、遠くにあるものは直接はかれないので、インフラ側にあるセンサや、他の車のセンサが取得したデータを通信で自分のところに持ってくる。あるいは、データそのものではなく、加工した情報・知識として自分のところに持ってきて活用するといったことが当たり前になってきています。これもＣＰＳやＩｏＴの最たるものです。

そこで出てくるのが、計測セキュリティ（Instrumentation Security）です。先ほど、フィジ

図表５



カルワールドとサイバーワールドの対応関係を揺るがす脅威について申し上げましたが、特にフィジカルワールドからサイバーワールドへ行くデータが歪められるケースに対抗するのが、計測セキュリティです。

少し詳細に見てみましょう（図表５）。「計測システムＳ（センサ）」は、カメラや自動車のレーダー、あるいは、後で御紹介するLiDARというレーザー光線を使ったレーダーや、超音波を使ったソナーといったものです。超音波というと潜水艦が有名ですが、車でも、駐車するとき周辺のモノにぶつからないようにするためのセンサなどで使われています。

「計測対象Ｏ（オブジェクト）」は、前にいる人や車、壁などです。例えばＳからＯまでの距離Ｘメートルをはかりたい場合、電波や光など、計測に用いるメディアがセンサとして働き、Ｘをあら

わす計測結果Zがあらわれてくることが期待されるわけですが、計測セキュリティにかかわる脅威として、次の三つがあります。

一つ目は、計測結果が実際と異なる。これは、先ほど言ったインテグリティにかかる脅威です。

二つ目は、計測できない。これはアベイラビリティにかかわる脅威です。

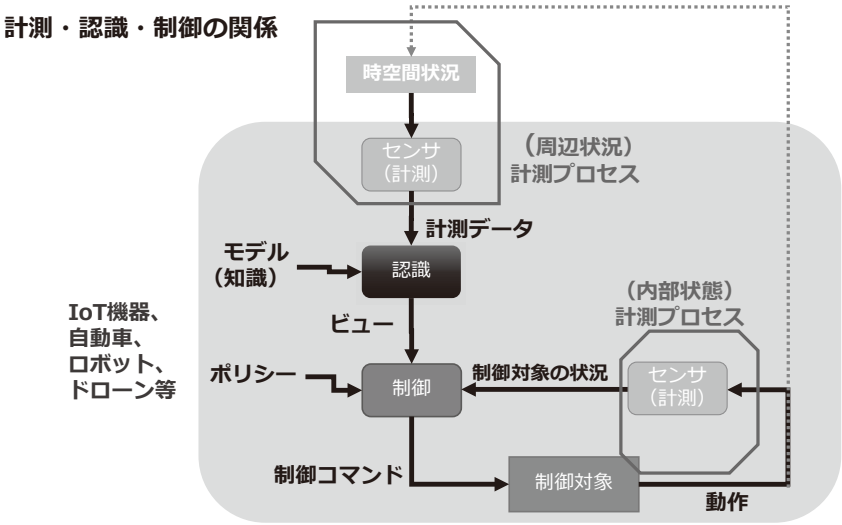
三つ目は、何を計測しているか暴かれる。例えばドーム型のセキュリティカメラは、どこを向いているのかわかりにくくして、「カメラがあっちを向いているから、こっちで何か悪さをしても大丈夫」といったことにならないようにしたいという用途がありますが、カメラがどこを見ているのか暴いてしまうということで、これはコンフィデンシャリティにかかわる脅威です。

つまり、計測セキュリティについても、一般のセキュリティで考えられる大きな三つの項目が成り立っているわけです。

では、実際の攻撃としてどのようなものがあるのか。センサが出す電波や音波や光そのものをおかしくする。また、センサや計測対象に電磁波や超音波や光を当てるということがあり得ます。あるいは、温度や照明、あるいは雰囲気、そこにある気体など環境を変えるということで、あらゆることが考えられるわけですが、こういったことによって、計測した結果が変わってしまったり、計測自体ができなくなってしまったりすると非常に問題です。

この計測セキュリティは、非常に幅広く捉えることができます。少し専門的になりますが、センサの中には、カメラの撮像素子やCMOSセンサといったイメージセンサからのアナログ信号を処理するアナログ回路、それをデジタル信号にかえて処理するデジタル回路のほか、ネットワークに

図表６



出すときにデータを暗号化して保護したり、通信の規格に合うよう変換するといったものが多段に入っています。攻撃者はその一つ一つに手を出すことができ、どこか一部分をおかしくしてしまえばいいわけです。

また、センサネットワークというものもあります。例えば、宇宙を観測するときに地球全体を望遠鏡にする、要するに、地理的にたくさん散らばっている小さい望遠鏡のデータを融合し、ある情報を得るということをしますが、たくさんのセンサが空間的に広がっている、場合によっては何キロメートルも離れたところにあるものも含め、計測システムの内部にネットワークがすっぽり入っている、こういうものもあり、計測システム（センサ）といっても多様です。

さらに具体化したのがこの絵です（図表６）。色塗部分は、自動車やロボットやドローンなど

の自律的な機器だとします。例えば、自動車は走っていると前後左右の周辺状況が時々刻々と変わってくるので、ここでは「時空間状況」と書いています。これをセンサで把握します。自分の車についているセンサだけでは十分でない場合には、先ほど述べたように、通信によって無線でどこかから教えてもらうこともありますが、この絵では省略しています。

センサから計測データを得ると、モデル（知識）をベースに、「何メートル先に人が出てきた」「前の車が急ブレーキをかけた」「カーブがある」といったことを認識します。人間もこういうことをしていますが、自動運転車ではコンピューターが行います。

認識すると、どういう状況（ビュー）なのかがわかるので、人をひかないように、あるいは前の車との距離を十分保つようにということで、ブレーキをかけたりハンドルを切るといった操作をします。そのような制御をするためには根拠となる判断基準（ポリシー）がなければいけません。つまり、ビューとポリシーから制御をどうするべきかということが定まり、制御のコマンドをブレーキに送ります。

車はそれに従って速度を落とす方向に行くわけですが、期待どおりにブレーキがかかっているのか、ハンドルが切られているのかなど、内部のプロセスを計測するという意味でここにもセンサがあります。もしも、まだ足りない、あるいは行き過ぎたという場合は、フィードバック制御といって、想定したところに落ち着くようにコントロールがなされます。

このように車の動きが変わることに伴って周辺状況も当然変わってきますので、点線で示したように、周辺状況を計測するセンサへの入力に当た

る部分も変わってくることになります。

以上が、抽象度の高いところで見た計測・認識・制御の関係です。

今述べたのは特に悪い人がいない場合ですが、では、「時空間状況→センサ（計測）」の部分が攻撃されるとどうなるのか。

セキュリティの研究に携わっている我々にとって、悪いことを一切考えなくても、セキュアで信用できるシステムがつくれれば理想的ですが、現実はなかなかそうはいきません。したがって、悪い人よりも先回りして悪いことを考えつつ、いかに倫理的に振る舞うかということになるわけです。もしも私が教えている学生や研究所のスタッフが悪さをしたら、大変なことになります。私自身もそうですが、技術がわかっているだけではダメで、どうすべきかというところの判断もきちんとできるようになっていかなければいけません。

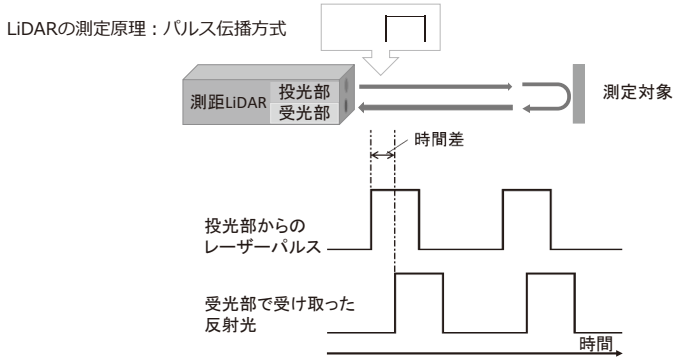
話が少し脱線しましたが、「時空間状況→センサ（計測）」の部分が攻撃されると、計測データも、ビューも、制御コマンドも、動作も当然影響を受け、おかしくなります。中身は故障に対して強くなっていたとしても、大もとのセンサが狂わされると大きな影響が出てしまうのは明らかです。

そこで、具体的に見てみたいと思います。LiDARに対する計測セキュリティの評価方法です（図表7）。

LiDARとは、投光部からレーザー光線を出し、測定対象に当たって跳ね返ってきた光線を受光部で受けるというもので、その測定原理はパルス伝播方式です。いわゆるレーダーですと、電波を出し、対象に当たって返ってくる電波を見て、出した電波と受け取った電波の関係から何らかの情報を得るという形ですが、それをレーザー光線に変

図表７

LiDARに対する計測セキュリティ評価方法



・Time of Flight方式（光の往復時間を用いる）に分類される

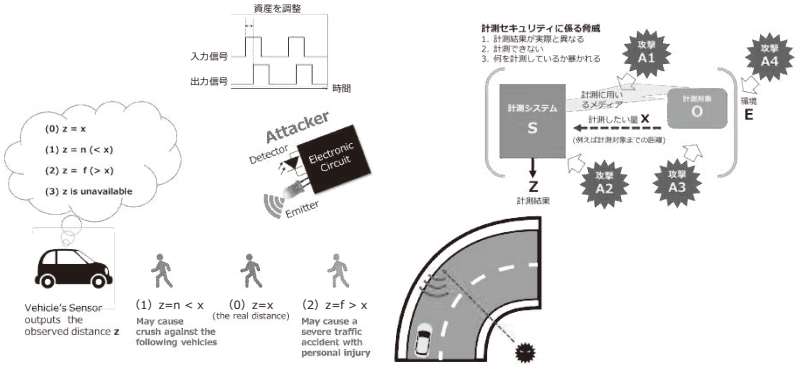
測定距離[m] $= \frac{1}{2}$(光速[m/s])・(時間差[s])

えたのがLiDARです。太陽光などの影響を受けにくくするため、普通は赤外線が使われます。

最近、安全運転支援や自動運転の目的でもこういうものがどんどん普及してきています。赤外線は目に見えないだけで、実際はそこかしこに飛び交っている状況ですので、そのままでいいのかという問題はまた別途あるのですが、それは置いておきます。

この図で見てみますと、横軸は時間です。時間とともに、強さがゼロに近くなったり、ある一定の強さになったりすることをパルスと言いますが、投光部からパルス光を出し、それを何度も繰り返します。そうすると、光には速度がありますので、瞬時に届かず時間差が生じ、反射光は少し遅れて受光部に到達します。光の速度に時間差を掛けると距離が出ますが、それは往復の距離なので二で割ります。これを、光が飛んでいる時間で

図表８



[1] J. Petit, B. Stottelaar, M. Feiri, F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR", Black Hat Europe 2015, November 2015.
[2] 相馬一樹, 勝本大介, 松本勉, "あるパルス LIDAR システムの反射光偽装に対する計測セキュリティ," 電子情報通信学会研究報告 ISEC2016-9, May 2016.
[3] 相馬一樹, 勝本大介, 松本勉, "測距パルス LIDAR に対する反射光偽装と計測セキュリティ," ハードウェアセキュリティフォーラム 2016, December 2016.
[4] Hocheol Shin, Dohyun Kim, Yujin Kwon, Yongdae Kim, "Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications", Conference on Cryptographic Hardware and Embedded Systems 2017, September 2017.

距離を見ることから「Time of Flight 方式」と言い、かなり正確に距離をはかることができます。

これは自動運転車が走っている絵です（図表８）。実際には(0)の位置に人が出てきたので、この人に衝突しないようにブレーキをかけたり、ハンドルを切ろうと考えます。ところが、アタッカーがLiDARに対して、光の検出器を使って電子回路で時間差をつくり、パルス光が遅れて出るようにしたら、事実としては(0)のところにいる人を、もっと遠くの(2)の位置にいるように誤認させることが可能であることが実験でわかりました。逆に次のパルス光が少し速く届くように偽装すれば、近くの(1)の位置にいるように見せることもできます。こちらも実証済みです。

右の絵のように、カーブのところで誰かが悪さをすると、車がだまされるということが起こり得るわけですが、そのやり方としては、計測システ

ム自体を攻撃したり、計測に用いるメディアを攻撃したり、場合によっては人に光を当てるということもあります。

もう一つ、例をお示ししたいと思います。先ほどは一方向だけ見ていましたが、三次元の方向にパルス光を出すのが一番高級なLiDARです。ある方向から反射してきたものを集積すると、点群と呼ばれるものが出てきて、何となく前方の車が見えるのですが、その点群が一部欠損するようLiDARに影響を与えたらどうなるのか見てみました。

前方を走っている車に赤外線をまともに返さないシールを貼りつけると、点群が欠損します。AIを使って車がいるということは把握しているのですが、点群が欠損すると車両の検出に失敗するということを先にサイバーワールドの中でシミュレーションし、それと実機が合うようにキャンパスの中で実験してみたところ、やはり検出に失敗するということがわかりました。これは、計測対象のほうに何か手を加えて車を見えなくしてしまうという攻撃です。

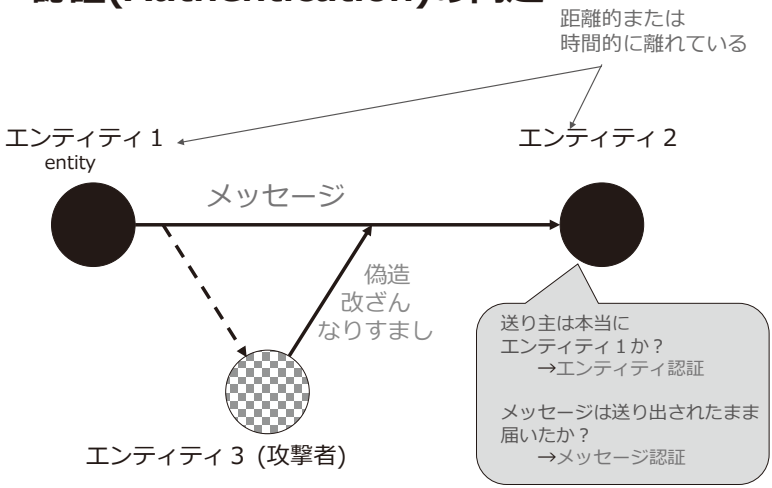
また連続フレームで点群を欠損させる実験では、車両までの距離について、ある一瞬だけだませるというのではなく、継続して八〇%以下で車両検出の失敗が起こり得ることが示されました。

さらに色調改変攻撃を受けた場合にどうなるのかということで、カメラにカラーフィルタをつける、フロントガラスに蛍光塗料を塗って特定の瞬間にブラックライトを照射するといった方法で見てみたところ、カメラに映る色が違ったものになったり、車線が検出できなくなるということが起こりました。つまり、アベイラビリティが低下し、事故につながり得るということです。

これらはほんの数例ですが、実際にこういった

図表９

認証(Authentication)の問題



ことがありますので、例えば自動車のある特定のセンサや、それにかかわるシステムのセキュリティを論じる場合には、きちんと評価の基準をつくり、その基準を上回るものをつくって安心して使っていきましょうということです。

三、ＩｏＴ末端機器向け公開鍵暗号技術の低消費エネルギーかつセキュアな実装

残り三つのテーマについては、イメージだけつかんでいただければと思います。

ここで言うエンティティは、人間や機械、プログラムを指します（図表９）。エンティティ１がエンティティ２にメッセージを送ったとき、送り主は本当にエンティティ１なのか、メッセージは書きかえられていないか、すなわち、なりすまし

や改ざんが行われていないか確認することを「認証」と言います。

また、エンティティ1はエンティティ2にだけメッセージを送りたいのに、途中でエンティティ3（攻撃者）に傍受、のぞき見、盗聴されたりするかもしれない。あるいは、自分が昨日書いた記録を今日見るときに、昨日書いたとおりのものかどうか気になる。これが「守秘」の問題です。

目の前にいる人であれば問題ないのですが、距離的または時間的に離れている場合、通信や記録において認証や守秘が問題になります。

したがって、貧弱なＩｏＴデバイスでも、暗号技術を徹底的に使っていかなければいけません。スマートフォンクラスのリソースであれば何でもできると思いますが、その辺にある小さなセンサは計算リソースがそれほどないので、末端のＩｏＴ機器にも暗号技術をセキュアに適用できるような「信頼の基点（Root of Trust）」が必要になります。小さい機器の中に入っているマイクロコントローラー、あるいは、SoC（System on Chip）という複雑な機能が載っているチップの中にSCU（Secure Cryptographic Unit）というものを用意し、それが安くできるようになると、世の中にあるあらゆるデバイスをつなぐＩｏＴの世界を末端から強くしていくことができます。

こういうものが必要だということを一〇年くらい前から言っていたのですが、内閣府主導の戦略的イノベーション創造プログラム（ＳＩＰ）という枠組みの中で、私が研究代表となって今年の三月まで研究を行い、結構いい技術を開発しました。それがＳＣＵです。ＩＣチップの中に組み込む暗号の計算をするエンジンと、そのエンジンが勝手に使われないようにするアクセスコントロールのソフトウェア・ハードウェアのメカニズムを

一体として持つものです。こういったものをどんどん適用していっていただけると、強くなるのではないかと思います。

また、宣伝になりますが、今、組み込み機器ではよく使われるようになってきた「楕円曲線暗号」と呼ばれる暗号の技術を、最小面積、最短時間、低消費電力でつくることにおいて、それぞれ世界記録を持っております。用途に応じてこういうものを組み合わせ、いろんな設計を自由にすることができます。

さらに、暗号の鍵や処理が内蔵されていますので、それがねじ曲げられたり外に漏れたりしてはいけません。先ほど述べた守秘性やインテグリティに対しても、ハードウェアレベルで十分にケアしたものがＳＣＵという技術として固められているところです。

四、ハードウェアの耐タンパー性のソフトウェアによる強化

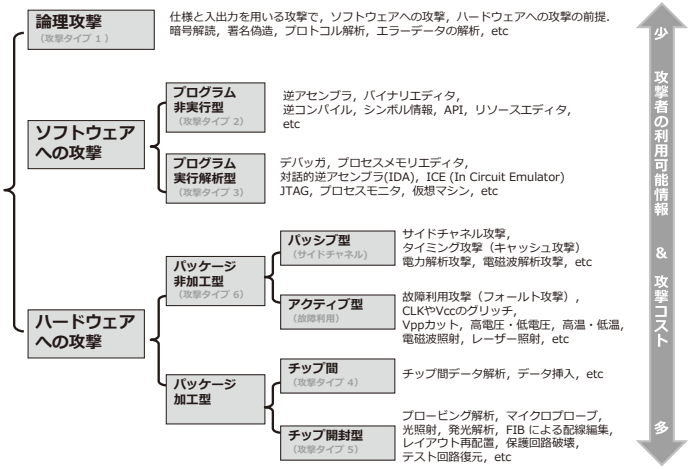
何かのシステムや、それを小さく一まとまりにしたものをモジュールと言い、それはソフトウェア・ハードウェア込みのものです。そういったものに対してアタックするときにどんな方法があるのかというと、論理攻撃、ソフトウェアへの攻撃、ハードウェアへの攻撃です（図表10）。この図のように、下に行くほど技術的難度やコストは上がりますが、得られる情報も多くなります。

論理攻撃は、仕様と入出力を用いて中を突き止めるなど、頭を使った攻撃です。

ソフトウェアへの攻撃は、ソフトウェアを動かしてみて、こういう入力をしたらああいう振る舞いをしたとか、あるいは、ソフトウェアが抽出で

図表10

システム（モジュール）に対する攻撃法の分類



松本 勉, 大石和臣, 高橋芳夫, "実装攻撃に対抗する耐タンパー技術の動向," 情報処理 Vol. 49, No. 7, pp. 799-809, July 2008.

きたら、ひたすらそれを読んで理解するといったことです。人間だけでというわけではなく、コンピューター上のいろんなツールやＡＩによってパワーアップした人間が分析するというものです。

ハードウェアへの攻撃は、究極的には、蓋を開けて中の半導体のチップを削るといったことですが、サイドチャネル攻撃や故障利用攻撃（フォールト注入攻撃）というものもあります。

皆さんは御家族から、「何か隠してない？」とか「嘘ついてるでしょ？」とか言われたことはありませんか。それは顔色などの微妙な変化によって見破られているわけですが、同じようなことが半導体チップや機器にもあり、漏れ出てくる何らかの変化を捉まえるということです。例えば、暗号の鍵を使って計算するとき、鍵の種類によって消費電力が微妙に異なる。あるいは、半導体が動くと中で光を発して電磁波が漏れてきたりします

が、その電磁波の漏れぐあいは中の計算にディペンドしているので、そこから逆算して求める。こういうものがサイドチャネル攻撃です。

故障利用攻撃は、人間で言えば、お酒を飲ませておだててしゃべらせたり、暴力で強制的にしゃべらせるといったことがありますが、装置に対しても、刺激を与えて情報を得るということがなされています。

アタッカーはこういう高度なことを行っていますので、それに耐えられるような技術が使われるようになってきているということです。

フォールト注入攻撃では、半導体のクロックを狂わせるとか、電磁波やレーザーを照射するといったことで、暴力に相当するようなことをやったりしています。これが一番手ごわい攻撃です。

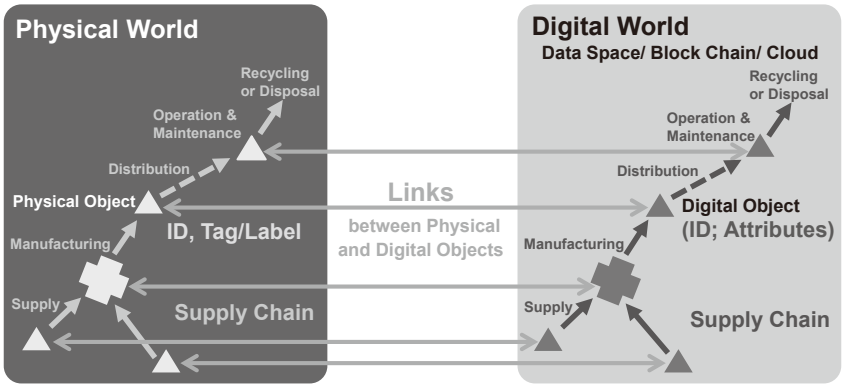
五、サプライチェーンのインテグリティを支えるモノの管理のための人工物メトリクス

最後に、人工物メトリクスについてお話しします。

例えば、一〇円玉は大量生産されていますが、よく見ると表面のパターンが一つ一つ違っています。アルミホイルも同様で、実は個性があります。これは人間で言えば指紋のようなものです。生体認証では指紋、顔、虹彩、静脈などを測定して認証しますが、その親戚の分野ということで、人工物のパターンを読み取ってマッチングするのが人工物メトリクス（Artifact metrics）です。この名前自体は私が随分昔につけたものですが、最近ようやく花開いてきたところです。

図表11

Object Management over Physical & Digital Worlds



© Tsutomu Matsumoto 2023

詳細は省略させていただきますが、かなりの精度で本物を本物と判断し、偽物をはじくことができます。

いろいろな用途に人工物メトリクスを適用しましょうということで、ISO 22387という国際標準規格が日本提案で昨年一二月に成立し、公表されています。「人工物メトリクス（Artifact metrics）」は国際的に認知された用語になってきており、今後の展開が必要とされます。

先ほどフィジカルとサイバー（デジタル）の間のリンクが重要だと申し上げましたが、こちらはサプライチェーンだと考えてみてください（図表11）。製造者が部品を調達し、製品をつくり、それを配送業者がビルや工場に配送し、そこでオペレーション、メンテナンスされ、必要がなくなったら廃棄またはリサイクルに回すという一連の流れがあります。

そのとき個体の管理はどうするかというと、普通はその個体をあらわすＩＤを用意します。そして、その個体の属性、すなわち、いつどこでつくったか、どこの材料を使ったか、その材料は強制労働で不当に製造されたものでないか、カーボンフットプリントはどうかなど、いろんな情報がＩＤとともに流通しなければいけません。しかし、肝心のＩＤと個体の関係が、実はＱＲコードを貼りつけているだけなど、簡単につけかえられてしまうものである場合がまだまだあります。これをもっと信用の置けるものにできないかということで、特に半導体など非常に重要な物品については、人工物メトリクスを活用することによって、サプライチェーンのセキュリティやインテグリティを強化していくことができるのではないかと思います。

雑駁で恐縮ですが、以上、私からのプレゼンテーションといたします。どうもありがとうございました。（拍手）

○増井理事長　一言でサイバーセキュリティと言っても、本当にさまざまな側面があり、しかも大変複雑な問題だということがわかりました。

それでは、質疑応答に移りたいと思います。御意見、御質問等いかがでしょうか。

すぐに出ないようですので、私から。

日本は以前から、サイバーセキュリティに対する対応が遅れているとか、弱いところがたくさんあると言われています。今のお話を伺うと、いろんな側面があるので一概には言えないかもしれませんが、世界的なレベルから考えて、日本の産業、あるいは国民生活一般について、サイバーセキュリティに対する対応はどのような状況にあるとお考えでしょうか。

○松本　日本はかなり安全だと思います。ただ、この前から毎日のようにChatGPTが話題になっているように、それらしいメールや文章をでっち上げる技術ができてきたので、これからまた危なくなってくると思います。今までの迷惑メールは、もともと英語や中国語だったものを機械翻訳で無理やり日本語に直したような、明らかにおかしい、稚拙な文章だったがゆえに見破ることができましたが、早晩、人間が見破るのは無理だという状況になると思います。

そうしますと、技術でどう対抗していくかという話になるわけですが、世の中には悪い人がたくさんいて、世界中のアタックしやすいところをアタックしています。要するに、最小コストでベネフィットを得ようと考えますので、そういう意味で日本がおいしいお客さんになっているかというと、まだなっていません。その点ではまだ安全なのですが、それは必ずしも強いからかどうかわからないという悲しい現実があります。例えばいろんな電子機器の中に入っている半導体チップは、昔は日本のものがほとんどでしたが、最近は電源のチップやアナログのチップ、センサのチップくらいになってしまっているので、アタックしてもしょうがないということで、すり抜けられている面もあります。

○質問者　ハードウェアの耐タンパー性のソフトウェアによる強化というのは、平たく言うとどんな考え方なのでしょうか。

○松本

半導体にレーザーを当てると、ゼロとか一のビットが反転するということがあります。

これは、コンピューターの機械語を人間が見えるようにしたアセンブリ言語の一部を取り出したものですが、一行が一つの命令で、その命令が連

図表12

New fault: instruction manipulation (IM)

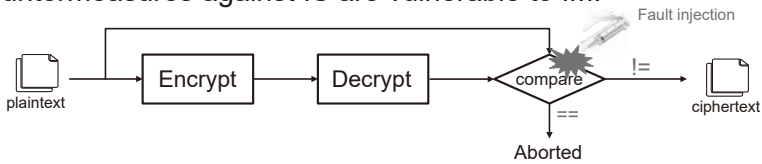
- Instruction manipulation faults are demonstrated:
  - with lasers.
  - on ARM and AVR devices.

#	Mnemonic : machine code
1	add r1,1 : 1001 0101
2	mov r2,r1 : 0011 1001
3	sub r3,r3 : 1110 1111

Instruction manipulation

#	Mnemonic : machine code
1	add r1,1 : 1001 0101
2	add r2,r1 : 1001 1001
3	sub r3,r3 : 1110 1111

- Countermeasures against IS are vulnerable to IM.



- No countermeasures have been developed yet.

なっているものがプログラムです（図表12）。

二番目の「mov r2, r1」は、レジスタと呼ばれるところにあるデータを別のレジスタにコピーしてくださいという命令で、「0011　1001」であらわされています。もしこれを「1001　1001」に変更することができると、「add」、すなわち、r1とr2のレジスタの値を足し算してくださいという命令に化けてしまいます。このようにフォールトを注入すると、プログラムとしては全く違うものになり、動かなくなるだけならまだいいのですが、情報を漏らしてしまうなど、いろんな困ったことが起きる可能性があります。

ある程度のセキュリティ対策が施されたプログラムの例ですが、フォールトを注入した場合にどのようなことが起こるか調べると、四〇九六回のうち五二八回アタックできてしまうとか、フォールトは検出できるもののアタックできないとか、

いろんなプロファイルを調べることができます。

こういうものをシミュレートすると、プログラムの書き方、ソフトウェアのつくり方によって、同じような強さの攻撃に対しても、打たれ強くなったり、そうでなかったりするということがあります。

ですから、重要な制御を担うプログラムにおいては、こういったソフトウェア上の工夫をすることも大きな対策の一つとして使えるのではないかということです。

○増井理事長　ほかにも御質問があるかもしれませんが、時間もオーバーしておりますので、このあたりで今日の「資本市場を考える会」を終わらせていただきたいと思います。

サイバーセキュリティと一口に言っても、複雑な対応があり、本当に御苦労が多いと思いますが、大変重要なお話だったと思います。

松本先生、どうもありがとうございました。

（拍手）

（**まつもと　つとむ・横浜国立大学大学院環境情報研究院教授**）

（本稿は、令和五年四月四日に開催した講演会での要旨を整理したものであり、文責は当研究所にある。）

松　本　　勉　氏

略　　歴

横浜国立大学　大学院環境情報研究院　教授

1986年東京大学大学院工学系研究科電子工学専攻博士課程修了、同年より横浜国立大学勤務。
2001年より同大学・環境情報研究院教授。
2018年11月から産業技術総合研究所サイバーフィジカルセキュリティ研究センター長（クロスアポイントメント）。

1981年から一貫して、基礎から実践に至る多様な分野のセキュリティ研究と高度人材育成・産学官連携に力を注ぐ。

1982年に「明るい暗号研究会」を４名で創設。
暗号と情報セキュリティシンポジウムSCIS、暗号学国際会議Asiacrypt シリーズ、電子情報通信学会の情報セキュリティ研究会、バイオメトリクス研究会、ハードウェアセキュリティ研究会の創設に貢献。
我が国の各種セキュリティ評価認証制度等の創設・運用にも貢献。

これまで、日本銀行金融研究所客員研究員、独カールスルーエ大学客員教授、日本学術振興会学術システム研究センター専門研究員、国際暗号学会IACR理事等を歴任。
現在CRYPTREC暗号技術検討会座長、内閣サイバーセキュリティセンターNISC研究開発戦略専門調査会会長、科学技術振興機構K Program「AIセキュリティ」プログラム・オフィサー等を兼任。

電子情報通信学会業績賞、第５回ドコモ・モバイル・サイエンス賞、第４回情報セキュリティ文化賞、2010年文部科学大臣表彰・科学技術賞等を受賞。