第 7回目　サイバーセキュリティー研究会
実施日：２０１９年1月３１日（木）
発表者：渡邊 創氏　国立研究開発法人 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 副研究センター長
発表テーマ：サイバーフィジカルセキュリティ研究センターの概要と戦略
会場：機械振興会館 5階　5S－2 会議室

本研究会メンバーである中島先生のご紹介で渡邊氏を今回の研究会の発表者として招聘した。氏が副センターとして最近就任されたサイバーフィジカルセキュリティ研究センターは、２０１８年１１月に産総研の研究拠点として設置されたもので、１２月１７日に記念シンポジウムが開かれた。氏からは研究センター設置の目的と研究の狙い、戦略についてご発表いただいた。

サイバーフィジカルシステムとは？
壁、階段、ビル、タワーの様な現物によって構成される物理的空間とコンピュータによってデジタルデータ化される事物及びネットワークによって構成されるサイバー空間が融合・連結されるいう事象に基づく体系的システム。IoT による物の（自動）接続化と現実世界を関連つけることで新たに価値が創造されるという近未来型アーキテクチャーが到来すると予測されている。

フィジカルセキュリティセンターの背景
大学、企業・評価機関、行政機関などセキュリティ政策の実現に向け、それぞれ努力は行われているが、機関ごとに個別によるバラツキがあり、研究という観点から総合的に知識・技術を結集したものはこれまで皆無であった。そこで政策側と評価・認証、認定などを行う機関との中間的窓口として、産総研によるサイバーフィジカルセキュリティ研究センターの設立に至った。センターのプロファイルは以下の通り。

研究者総数　１１５名（１２月１７日現在）
産総研所属研究員８８名＋外来研究員（含む学生）２７名

研究拠点：３箇所（臨海副都心センター、筑波センター、関西センター）

センターの主な狙い
サイバー攻撃手法の変化や対策上の盲点に伴い、これまでに国が定めるセキュリティレベルの基準だけでは攻撃脅威の正確な把握や判断が難しくなっている。そこで新しいセキュリティ評価方法、保証スキームの開発と実装に向け技術的な研究を行うことを主な目的と

した。

臨海副都心
高機能暗号研究チーム、暗号プラットフォーム研究チーム、セキュリティ保証スキーム研究チーム、ハードウェアセキュリティ研究チーム

筑波
インフラ保護研究チーム、ソフトウェア品質保証チーム

関西
ソフトウェアアナリティクス研究チーム、連携研究室（住友電工との連携研究）

質問・コメント（一部抜粋）
Q:ご紹介いただいたプロジェクトは基本的には、産総研がこういうものをつくったという研究部門と捉えている。その研究部門をこうして集めることの意味について聞きたい。価格や用途上の制限、スコープが広すぎるなど様々な制約があり、集める必要はあるのか、又集めることのメリットはどれが一番中心なのかということを教えて欲しい。関連でアメリカのカウンターパート的なものはあるか。
A:ハードウェアのセキュリティから始めなければならなかったが、産総研では全然足りていなかったところがあった。いくつか大学の先生の良い研究室や論文賞を取ったものなど光るものはあるが、それぞれ別々にやっているという感がある。一緒にやりたいという動きはあるものの、どこまでやるかというと、NEDO のように分担で行うという感じであった。そういう場を作ることが主な目的になっていると考えている。海外だと、米国だと NIST がこちらのフィジカルサイバーセキュリティと似たような活動をしているところがある。ただ、どちらかというと政府の機関で、自分のところで新しいものを造るというのはあまり強くなく、ガイドラインや標準を作るというのが主体である。独自でやるというのは海外でもなかなかないと思う。こちらでもガイドラインを作れるかというとそうはいかず、IPA など国の機関としての形が入ってくる。そういったことから、連携しながら海外でやっているようなことも実現していきたいと考えている。

Q:２０３０年になると自動運転のシステム開発が工場などのシステムと繋がり、色々な悪さをする恐れが出てくる。これを踏まえると、製品の Product Liability や規制についても全く違う次元で責任を考える必要になりなかねない。先ほどのお話の中で、セキュリティ保証スキームの研究チームをご紹介いただいたが、今後どのような枠組みが提示されていくのか全く想像つかない。どこかで線引きするものはあるか。

A:一つのやり方としては、情報というものをコントロールしてやりとりさせるようなところ。その形がいいかどうかは別にして、それこそ情報銀行のような話とかありますが、どういったところでこの情報が扱われるべきかというようなところも、しっかりとうまくコントロールしたような状態でやりとりされるようなところをまずきっちりと決め、その中でどのように守っていくのかということ。そのようにある程度絞っていかないと、「この情報はどこに行くか、よく分からない。全部可能性があるから」というようなところからやると何もできない。何かあったときでも、それをうまく排除できるとか、そういったものも必要かと思っている。特に IoT になると、センサーは壊れるので、何十年もほったらかしにされるものまであるので、そういうところもうまくやりながら、全体としてはできるだけ堅牢に動くようなシステムのようなものも一緒に考えないと。セキュリティだけではなく。
Q: 野放図に 2020 から 2030 に行くのではなく、秩序を持った展開がないといけない。
A:秩序を持った展開がないと、怖くて使えない。

情報統制と物理制御の違いによる制約に関して
Q: この話は、正に CCC（カルチュア・コンビニエンス・クラブ。T ポイント）などのポイント系個人情報収集でやっていることと言える。この肝は何かというと、ほとんど全てをマイクロサービス化して、マイクロした部分を疎結合にしてしまえば、本来であれば情報の持っているものは隠蔽したままうまく使えることだ。どころが情報を全部握ってしまったら、個人でも全部仕切ることができる。だから「2020 年頃まで？」と資料に書いている絵は、実はもう既に半分ぐらい「2030 年頃には」という方向に行ってしまっているという認識はいるのではないか。
A: 今のところは上のほうだけでぐるぐるぐるぐる、上のほうでこうなりながらやっている感じかとは思う。クラウドの人たちが、実はあれはあまりなく、それぞれのシステムでは CCC であったり、Facebook であったり、Google であったりしていて、それが実はそれぞれ下のものを持っていて、上のものが一つになっているような絵がいくつもあり、それぞれが実は相当大きく、クラウドのところに全部持っている状況だと思う。

Q:そうだとすると、既に日本はもう 3 周ぐらい遅れている状態だ。この流れの中で情報の統制というか制御というか、そこに対し、どのようなビジョンとかがあるのだろうという疑問を持った。情報を送信する部分とか、解析する部分とか、蓄積する部分とか、それを業者に対しフィードバックする部分。もしくはシステムに対しフィードバックする部分、全てに対し、いま産総研さんというか、ここでやられているプロジェクトの中で、どこに使えるテクノロジーがあるから、この部分は、テクノロジーはどのようにしたらいいかとやられていると思うが、どんな感じか？そのビジョンを明確に出せるのだったら、きっと苦労はないなとすごく思うが、今のところどんなところか？
A:　情報統制と機械統制それぞれの一つのパスを描いており、その中で特定の部分（データ

蓄積部分）がどうい動いているのかモデル化することはできるとは思う。ただどうすれば肥大化させないのか、ある一定のところに保ってしまうことを防げるかどうかによる。

Q: 聞きたいのはそこを保護するための仕組みとか、収集から蓄積、蓄積からフィジカルへのフィードバックの部分を保護するための暗号とかというようなことを含めた全体の流れに対するビジョン。
A:それ自体はそこで何が守られるのかがあり、それに基づき、例えば暗号を使うとか、そういった形でやることになると思うが、実際にはなかなか難しい。

Q:欧米では十数年前からアーキテクチャフレームワークを十数年前から取り入れ、データはハードウェアの構成についての記述や描写が基準化されている。日本ではそのような視点がない。この CPS の話ではシステムが連接されたことを前提にしているが、アーキテクチャーフレームワークは、不具合やサイバー攻撃が起こった際の原因や再発防止の対策には必要不可欠である。その整備がないまま行くのは危険だと思うがいかがか？
A:仰る通りで、データをやりとりするとき、言語が違うとそもそも全然つながらない。その中でどういったことが信頼でき、渡されているのかがちゃんとできるような仕組みをそれぞれのところでつくらないといけない。全部つくれるかというと一つのところではできない。考え方であるとかそういったところは示していきたい。

データ構造・フォーマットに関して
Q:システムは、結局データ構造が決まれば何とかなるのだが、その肝心のデータ構造がない。IoT はものによってデータ構造が違うため、トラブルが起こると一番危ないのはデータをトランスファーして正規化する部分ということがある。いまこの流れの中でやっていると、たぶん正規化がすごく大きな問題になると考えられる。これは産総研さんがやるべきなのかどうかは分からないが、産業の世界の中で情報交換を行うとなると、恐らくそこに一番近いのは産総研さんという見方になると思う。データ構造についてはどうお考えか？
A: 全部データ構造まで統一するのは無理がある。難しいが、データを正規化しやりとりできるような形として考えられている案の一つは業種ごとの対応である。例えば、電力や防衛産業とか業界の範囲の中で統一した形でできるものを目指ざすという動きがある。ビルの中だったらビルシステムの中でやりとりされる情報については、部品のところまでこういった形でやりましょうとか、そういったことはできるかもしれない。情報のやり取り全体の部分を統一できるかどうかは別として、ある部分については対応できるようにする、というものが求められているのではないかと思う。

Q:最初の話で、日本がサプライチェーンから弾き飛ばされるという懸念があった。海外では、北米や欧州のように地域ごとにデータの相互のやりとりを行うための枠組みがあるが、

日本には存在しているのか？日本では何かしようという動きがあるか？
A: そもそも基本的にないような気がする。誰が決めるのかというところもないと思う。ISO/IEC では、IoT の SC があるが、枠組みを決めるというレベルでは全然ない。
人によって言葉の解釈が異なり、その中でもガイドライン的なものはつくりましょうというようなところはある。本当のデータフォーマットまでは全然行かないが、こういうときにはこういう観点でこういうことをしなさいというようなところは、いま議論が始まりつつあるレベルである。ISO でもたぶんデータフォーマットまではつくれない。
業界団体がベースの取り組みとか、そういったところで何かするのかなという感じはするが、まだそこまでは議論できていないという認識である。

IoT、アプリケーションのオープン化
Q:IoT による自動接続化を巡り、アプリケーションのオープン化について賛否両論があるが、何がメインターゲットになっているかこれまでに何か議論があったか。
A: システムにおける議論を行う際に共通するのは、我々を含めてそれぞれところで何を確かめておく必要がありそれについて対応するというものである。つながることを前提とし、どの状況で、どういったアプリケーションや、どういうサービスができるのかといったユーザーニーズに合わせたオーダーメイドという話は実はあまり行われていないというの気がする。まずはやろうとしているという点にご理解いただければと思う。おそらく皆様の方がご存じかと思うので、何かあれば、そちらほうから言っていただけると私も勉強になる。

研究所としての位置づけ、方向性、研究者の分野的特徴など
Q: 海外で求めている分野で実績を上げている研究者を迎え入れる計画はあるか？
A: 機会があれば沢山招聘したいと考えている。
Q: 産総研では特に大学のほうに何らかの形で還元するとか、例えばあるリサーチャー用にリサーチャーが今後の研究のために何かするというアイディアはあるか？
A:　海外の大学は企業にお金を出してできるが、産総研はそもそもそういうところに出すお金がないところが一番の問題である。一方で産総研の仕組みとしては、大学と連携するような仕組みを作っていある。どう作るかが今後の検討課題だと思うが、産総研が大学の場所の一部を借り、そこに出店のようなものをつくり、産総研に大学の先生をお招きし、産総研と一緒に研究するようなオープンイノベーションラボラトリと言っているものが、いま 8 個ぐらい各大学にある。そういった形で大学と密に連携するような仕組み自体はある。ただ海外のようにお金を持って Institute のようなものを創るというのはなかなか難しい。研究費の一部を寄付金のような形で口座を開設し、大学と連携するというものを考えている。
Q: 研究者ということでセキュリティ政策上の方向性や諸問題について提言する機会はあるかと思うが、その際に国や役所から何らかの圧力や制約を受けるリスクはあるか？
A: 技術的な部分については、包み隠さずに現場の役所の方々に報告することはある。それ

が反映されるかどうか、役所の中の判断、あるいは政治家が出てきたりしたら、またそれで問題がいろいろ大きくなったりすると困るので、「技術的にこういったところはこうですよ」というようなところは、機会があるごとには言っているのが現実である。現場の若い人たちのところではオフィシャルにドーンと言うのはなかなか難しいかもしれないが、話をしに行くこと自体は問題ないと思っているので、それ自体はやっていっていますし、これからもやっていくつもりでいる。

Q:集まっている先生方はどちらかというとセキュリティ系の特に暗号系のとんがった人たちが多いが、その一方でセーフティとかリライアビリティとか工学系というのか、ものづくり系の人たちをどのように組織化しようとされているのかについて聞きたい。
A: ソフトウェアの部分の研究者は今まではセーフティとかリライアビリティをやっていた者が多い。セキュリティ以外のところは全部はできないとは思うが、そういったところも含め、やっていきたいと思っている。例えばAIの品質保証は、実は産総研の中に人工知能研究センターというものがあり、そちらの研究者と一緒にやっているプロジェクトである。そちらにAIの専門家がいるが、どちらかというとソフトウェアエンジニアリングなどをベースにした研究が中心で、リライアビリティやセーフティといったものもターゲットにして行おうとしている。うまく連携しながら何らかのアウトプットを出していければと考えている。

Q: この間大津のSCISに行った際、とんがった暗号の人たちが本当に暴れられるところというか、安心していろいろなとんがった実験ができるようなところを、ぜひ産総研さんでフィールドをつくっていただけると、彼らとしてありがたいと感じた。
A:せっかく世界レベルでプレゼンスの高いグループができていて、そこはどんどんとんがらせる方向で産総研としても了解している部分があるので、おっしゃるように暴れられるようにしたいと思う。ありがとうございます。