サイバーセキュリティ戦略本部
研究開発戦略専門調査会
第１回会合　議事概要

１　日時
平成 27 年４月６日（月）　16:30～18:35

２　場所
フレンドビルディング７階会議室

３　出席者（敬称略）

（会長）	後藤 滋樹	早稲田大学理工学術院教授
（委員）	上野 裕子	三菱 UFJ リサーチ&コンサルティング株式会社 政策研究事業本部 経済・社会政策部 主任研究員
	小松 文子	独立行政法人 情報処理推進機構 情報セキュリティ分析ラボラトリー長
	小山 覚	NTT コミュニケーションズ株式会社 経営企画部 マネージドセキュリティサービス推進室 担当部長
	新 誠一	電気通信大学 教授
	神成 淳司	慶應義塾大学 准教授
	名和 利男	株式会社サイバーディフェンス研究所 理事／上級分析官
	松原 実穂子	インテル株式会社 サイバーセキュリティ政策部長
（外部発表者）	鍛 忠司	株式会社日立製作所 研究開発グループ テクノロジーイノベーション統括本部 システムイノベーションセンタ セキュリティ研究部 部長
	西垣 淳子	経済産業省 製造産業局 ものづくり政策審議室 室長
（事務局）	髙見澤 將林	内閣サイバーセキュリティセンター長
	藤山 雄治	内閣審議官
	谷脇 康彦	内閣審議官
	徳田 英幸	サイバーセキュリティ補佐官
	三角 育生	内閣参事官

（オブザーバー）　内閣官房情報通信技術（ＩＴ）総合戦略室
内閣府
警察庁
総務省
文部科学省
経済産業省
防衛省

4 議事概要

（1）谷脇内閣審議官挨拶

（2）研究開発戦略専門調査会について
事務局から、資料 1、資料 2、資料 3 に沿って説明。
その後、後藤委員を会長に互選。

（3）IoT セキュリティの進め方について
事務局から、資料 5 に沿って説明。

（4）IoT セキュリティに関する発表
資料 6-1～6-4 に沿って、以下 4 名の方からそれぞれ発表。

①徳田補佐官
②小山委員
③鍛部長（日立製作所）
④西垣室長（経済産業省）

（5）IoT セキュリティに関するご議論

○（新委員）まず、徳田先生の発表資料 6-1 の P.10 にあるレイヤ毎、P.23 にあるアプリケーション分野毎のセキュリティレベルの話に関し、制御システムには IEC62443 という国際標準がある。日本では、一番上のマネジメントレベルとなる CSMS 認証制度を JIPDEC（一般財団法人日本情報経済社会推進協会）、一番下の EDSA というデバイスレベルの認証を私が理事長を務めている CSSC（制御システムセキュリティセンター）が対応している。また、今年度から SSA というシステムレベルのセキュリティのパイロット認証も CSSC で始める予定。日本は突出して IEC62443 を進めているので、徳田先生御指摘の分野毎のすり合わ

せというものは一つの柱になるかと思っている。

あと、皆さんの話に明示的に出てこなかったが、現在 2000 年頃と随分状況が違う点は、ネットワーク通信が IPv6 になってきているということ。IPv4 は御承知のとおり IP アドレスが数十億、すなわち 10 の十乗のオーダーであるが、IPv6 になると大体 10 の四十乗のオーダーの数になる。これだけ多くのアドレスをどうやって把握するかという根本的な数の問題が出てくる。それが、発表で御指摘のあった IoT のモノの管理ができるかというガバナンスの問題にもつながってくる。

また、数千万台のスマートメーターを各家庭に配ることになると、攻撃側はどのような脆弱性、セキュリティホールがあるかを手元で調べることができる。ルーターの脆弱性の話も出てきたが、スマートホームも同様である。いつでもモノを購入できて自分の手元で調べることができる。これが今までの 20 世紀のプロが管理してきた機器のセキュリティと異なる IoT の本質的な問題であると思う。

それから、小山委員の発表の中で、IoT の特徴として機器が 10 年以上使われるという説明があったが、従来の IT 機器にも 10 年以上使うものがある。銀行でもメインフレームで COBOL が動いている。これら古いものは皆ファイアウォールを設定する形で使用している。このような形が、小山委員が説明された Intranet of Things という、ある管理されたネットワークの中で機器を使うという発想につながってくる。

西垣室長からは、制御機器は 24 時間 365 日使うものであるという説明があったが、IT 機器でも例えば円の決済などのために、24 時間 365 日決して途絶えることなく稼働が必要なものもあり、制御機器特有の話ではなく、情報機器全てについて今のような問題を考えていかなければいけないと思う。

更に、今や、CAD（Computer Aided Design）という形で、コンピュータを使って皆が 3D のデータを作って、その気になったら 3D プリンタでモノを作る時代に入ってきている。Web 系の話も含めて、これを UGC（User Generated Contents ユーザー生成コンテンツ）という。有名な犯罪としては、昨年の 5 月に大学職員が 3D プリンタの設計データに基づいて拳銃を作ってしまった例がある。今まで設計して製造するというのは、プロフェッショナルのエンジニアまたは工場の中だけで行われてきたことであるが、今の時代は誰もが設計者になって製造できる。そのようなことを明確にしたのが昨年の事件であったと思う。それらを考えていくと、ソフトウェア、情報、色々なものが誰かによって改ざんされたり、このような素晴らしい製造システム、または皆さんの安全を守る快適なシステムというものが、いつ乗っ取られて、思いと違う方向に使われたりするといった点も非常に大きな問題であると思う。

まとめると、1 点目は IP アドレスが 128bit 化され、莫大な数に増える IP アドレスを皆で利用しようとしているが、逆にリーチ（到達）することが大変な状

況にある。管理ができない。２点目に機器が悪い人の手元に渡るということ。３点目に、UGC という形でユーザーがどんどん製造システムに入ってきて好きにいじることができる体制になりつつある。これらの３点に対してどのように対応していくか。先ほど御紹介した IEC62443 がセキュリティ基準の一つの尺度にはなるが、ユーザー作成コンテンツが広がっていく点、IP アドレスが増えていく点については対応できていないということに留意が必要。

○（後藤会長）昔、制御用コンピュータと、いわゆるデータ処理用コンピュータは別のものであった。制御用コンピュータがデータ処理用と置き換わった実例は電話の交換機。電話の交換機は電子交換機といっていても実は独自の制御用コンピュータであり、通話路は電子化されていないものが長い間使われていた。その時のアーキテクチャは独自設計で国産品であり、パッケージレベルつまりプリント基板まで互換で、20 年間使うという想定で設計されていた。ある会社の基板を抜いて他社の交換機に入れても動くという形で運用されていた。そのようであったものが、今日では IP 電話というものをサーバーで動かすようになっている。

かつて工場においては、イーサネットの普及前に MAP（Manufacturing Automation Protocol）、TOP（Technical Office Protocol）といったものが提案され、実物もあったが、どれぐらい使われたかというのは先生方御存じのとおりである。

○（名和委員）皆様の発言を聞いて分かったことは、もはやセキュリティの観点では手遅れだということである。このような方法で守っていくことが不可能であると分かったということを本日議事録に残していただきたい。何をしても今の制度の仕組みでは分野横断的に対応するのが厳しく、法律を変えないと厳しいところがあることは、やはり目をつぶらないようにした方がよいかと思っている。

今日の発表の中に、悪意のあるデバイスを見つけるという技術に関する関心事項がなかったことを少し不思議に感じた。諸外国、特に先進国においては、ハードウェア・トロージャンに関する防御技術にかなり予算を計上して取り組んでいるが、日本はそういうものがあまり見られない。

資料 5 の「ご議論いただきたいポイント」の「セキュリティ技術の開発・実証はどうあるべきか」というところで、今日の話を私なりに考えた結果としては、悪意のあるデバイスをどのように見抜くかということで、その技術開発は１社では無理であり、やはり公的な機関が行うべきではないかということである。

○（神成委員）例えば農業分野でいえば、自動運転が数年先には実用化されようとしている中でのセキュリティ・バイ・デザインの考え方。あるいは健康医療でも、健康データの取り扱いがどのようになるのか。来週には予約が始まる Apple

Watch もそうであるが、これらのデバイスで取得したデータは、それぞれのベンダーのサーバーに蓄積され、個々人のものとなっていない。

既にビジネス化されているものは、こらから対応することが無理なものも多くなっているのは事実であるが、少なくとも我が国の取り組みの中で、いかにセキュリティ・バイ・デザインの考え方を、研究開発あるいは各省の取組の中に入れておくのか、体制をどのように構築していくのかを考えていかなければならない。

農業では、UAV（無人航空機）を用いた研究開発が数多く進められている。総合科学技術・イノベーション会議でも多く提案されているが、セキュリティに関する検討が遅れている。農機の自動運転にセキュリティリスクがあれば、農機が暴走する可能性もある。北海道の圃場では、農機の協調運転の実験が取り組まれている。地方創生 IT 利活用推進会議や近未来実証特区の議論においても、UAV や自動運転の検討が進められており、ここでもセキュリティ・バイ・デザインの考え方をどのように適用するのかを考える必要があるのではないか。

○（松原委員）資料 6-4 経済産業省御説明資料「IoT によるものづくりの変革」の P.13 の「課題の整理」について質問したい。課題として、デジタルものづくりやデータ蓄積・解析に関する人材の不足、国際標準化やサイバーセキュリティへの対応の必要性等が挙げられているが、ここに出席している委員、日本の学者や産業界がこれを受けてどのように動いていってほしいか、経済産業省側の御期待について伺うことができればと思う。このような動きは 2020 年のオリンピックにも絡んでいると思う。経済産業省として 5 年後を見据えて、大体これくらいまでにはここの部分は対応させたいという、目標やマイルストーンをお持ちだと思うので、差し支えない範囲でお話をいただければと思う。

○（経済産業省 西垣室長）このページは、4 月 3 日に産業構造審議会の下にある製造産業分科会に提出した資料であり、正にこれから課題の整理をし、どうするかを考えるところである。今動きがあるもののみ簡単に御紹介する。

IEC の国際標準化検討の中で、Factory of Futures、すなわちスマート工場のあり方論というものが始まったところであり、これが 5 年以内には規格づくりのレベルまで進むであろうと考えられる。そして今、セキュアなネットワークの必要性といったものを日本から提案しているところである。新先生が進めている制御系の IEC 規格のお話があったが、そういったものがスマート工場の中に埋め込まれていき、必須要件となっていくというような姿を進めていきたい。

標準化の世界は、我々政府機関から見ると非常に近い政策分野なので、その辺りからまず取組を始めている。セキュリティに対しては、このような場において、皆さんで議論をされている中に我々としても一緒に課題を共有していくようなことができたらと思っているので引き続きよろしくお願いしたい。

○（小松委員）小山委員が紹介した中で、CCC（Cyber Clean Center）の話があったが、これは国際的にも非常に先進的な例である。利用者の PC がボットウイルスに感染しても、利用者に直接被害は発生しない。しかしボットがネットワーク経由で別の利用者に被害を及ぼしてしまうのであるが利用者自身が対策をするというインセンティブがあまりない。そのため、このような官主導で民と一緒に行う活動というのは重要と思っている。

CCC は PC のユーザーが対象であったが、IoT では IT をよく知らない方も使うことになるので、CCC よりも利用者の IT リテラシーのレベルを更に考慮した活動が必要になると考えている。

CCC 自体は素晴らしい活動であったとが、一つだけ懸念しているのは、あなたの PC にはボットウイルスが入っているので CCC クリーナー（駆除ツール）をダウンロードして対策してくださいというメールを出しても、実際は 5 年間の活動の中で、30 パーセント前後の利用者しかダウンロードしないという実情があり、更にはダウンロードした後に対策したかどうかもわからなかったということ。技術的には対策を提供しても、利用者にリーチ出来たのは 30 パーセントだけであったことから、利用者に対して注意喚起をどのようにするかという手段が重要と思っている。IoT になると特に IT に弱い方達も対象となることをよく考えていかなければなければならない。

もう一つ細かい点だが、技術的に 100 パーセント確かなものというのはないので、新たな脆弱性などが発見された際に利用者にリーチできるような仕組みが欲しい。Web カメラの脆弱性が発見された際、PC のように自動的にアップデートができたので、かなりリーチできてはいたと思う。しかし、全くリーチできないようなネットワーク機器というものが沢山出てくると思うので、保守の面でのアップデートを自動化する等の方策が大変重要になるのではないかと考えている。

○（後藤会長）CCC は実際のボット対策にも有効であったが、ハニーポットのデータを学会の活動等に用いることで、その後の日本での研究が進展する一つの要因となった。小山委員にも当時非常に尽力いただき、今活躍している方でもお世話になった方はずいぶんあるのではないかと感謝している。

正に御指摘のあったガバナンスや、誰に連絡すればよいのかという点について事例を紹介する。私は IP アドレス等を割り当てている JPNIC（日本ネットワークインフォメーションセンター）の理事長を務めているが、そこで割り当てただけでなく正しく使われているかの確認について、JPRS（株式会社日本レジストリサービス）と共同で取り組んでいる。DNS（Domain Name System）は規格上、プライマリとセカンダリの 2 つが動いていないといけないが、lame delegation といって、有効でないセカンダリがあったり、セカンダリを動かして

いなかったりする方が結構世の中にいる。そういう方に警告を出すが、どれだけ有効か。我々が警告したが正しく受け取ってもらえなったり、運用を他に委託している人には連絡しても何のことか話が通じなかったりということがあり、大変に苦労する。

今日はガバナンス等、色々指摘があった、一体誰に責任があるというか対応してくれる期待感が業界に対してあるのに、言っても難しいということ。IP アドレスやドメイン名の連絡先は「WHOIS」というドメイン名登録データベースで一応管理しているが、情報がなかなか現行化されていない方もあり、連絡が取れないという状況がある。今日御指摘があった、誰が何をするのかということは非常に実際の世の中で重要かと思う。

○（新委員）今の問題は、プライバシーの問題にも係ってくる。「WHOIS」を悪用する攻撃も数多くある。

○（後藤会長）この件は、通信の秘密にも係ってくる。「WHOIS」のプライバシーは、国際的にはより守る方向で進んでおり、日本でも議論している。私の米国の知り合いが Privacy Aware Measurement（プライバシーを意識した測定法） という形で、ネットワークの測定を実現する提案をすると言っていた。パケットの中を見ようとすると DPI（Deep Packet Inspection）だということになり、問題視される。これ以上は議論が長くなるのでこの辺で止めるが、色々皆さん御苦労されているところだと思う。

○（上野委員）資料 5 の「新たな製品・サービス群によるビジネスの創出や既存ビジネスの高度化を図る方向に向かうと見込まれる」で、今後つながりの増加が見込まれることが示されている。本日、利用者がよくわからないままつながってしまうことによる危険性という話を伺った一方で、つながっていかないと競争力もなくなるという状況下にありながら、つながることができないという日本の姿も伺った。大手・中小企業、あるいはものづくりを始めとする色々な業界を含め、日本の産業界が実際どのような状況にあるのか、現在の実態がわかるとありがたい。

以　上