産業サイバーセキュリティ研究会WG1
『第2層：フィジカル空間とサイバー空間のつながり』の
信頼性確保に向けたセキュリティ対策検討タスクフォース
（第1回）議事要旨

1．日時・場所

日時：令和元年8月2日（金） 10時30分～12時30分

場所：経済産業省　別館1階104各省庁共用会議室

2．出席者

委員　　：松本委員（座長）、青木委員、石原委員、伊藤委員、岩崎委員、荻野委員、梶屋委員、神余委員、
北澤委員、戸枝委員、西貝委員、野口委員、松元委員、渡部委員

オブザーバ：内閣官房　内閣サイバーセキュリティセンター、警察庁、総務省、厚生労働省、
国立研究開発法人産業技術総合研究所、独立行政法人情報処理推進機構、
技術研究組合制御システムセキュリティセンター、独立行政法人製品評価技術基盤機構、
一般財団法人電気安全環境研究所、電子商取引安全技術研究組合、
一般社団法人日本自動車工業会、一般財団法人日本情報経済社会推進協会、
一般財団法人日本品質保証機構、一般社団法人JPCERTコーディネーションセンター

経済産業省：大臣官房サイバーセキュリティ・情報化審議官　三角審議官、
商務情報政策局　奥家サイバーセキュリティ課長、鴨田サイバーセキュリティ課企画官

3．配付資料

資料1　議事次第・配布資料一覧

資料2　委員名簿

資料3　本タスクフォースの議事運営について（案）

資料4『第２層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討
タスクフォースの検討の方向性

資料5　セキュリティに関する標準化動向

4．議事内容

事務局から、資料3,4による本タスクフォース（TF）の議事運営および検討の方向性について説明、神余委員から、資料5に基づき説明いただいた後、自由討議を行った。委員からの意見は以下のとおり。

●問題意識等について

・ サイバー空間とフィジカル空間のつながりという、これからの社会で最も重要なところに手を付けられたことに大きな期待。これだけのものをつなぐとすると、既存の技術の寄せ集めではなく新たな枠組みが必要。サイバー空間の IoT の世界とフィジカル空間を、まだ分離して捉えており、技術的な話とマネジメントの話も分離している。さらにマネジメントでもセキュリティマネジメントと一般マネジメントで分離。今日の資料でも、技術 IoT セキュリティの観点がほとんどで、他の観点があまり出てこない。これまでのサイバー空間の技術者の技術論に収まってしまうのではないか懸念。これからの社会が、どのような IoT 技術を組み込もうとしているかという技術トレンドや、産業トレンドが、大事ではない

か。

・ 欧州のサイバーセキュリティ認証フレームワークは ENISA が中心としてやっているが、国際標準化機関としてプレゼンスを発揮すべきという意見から欧州委員会のトップ等を交えてハイレベル会合を行っている。Cybersecurity Certification Framework で議論の中心になっているのは、各国がバラバラなフレームワークを作ることは絶対に避けたいということ。一方で、国際的な流れともマッチングさせなければならないため、情報収集、分析の状況が続いている。欧州の大手の関心の高いメーカが、域外産業界、特に日米の産業界の声を反映して意見していることもあり、ヨーロッパで活動している人間を通して我々の意見が段々反映されるというメカニズムができつつある。

・ 医療機器の場合、複数の機器がネットワークで繋がった際、それぞれのデータの処理の方法や通信仕様が統一されておらず問題になることがある。相互運用というアプローチがここ数年重要になってきている。

・ ルータに SSID を 2 つ設定してそれぞれを VLAN で分けるという提案があり、SSID を 2 つ設定できるものが産業用にはあるが、安価な家庭用だとあまりない。また、VLAN を設定しようとしたとき、IoT 機器が VLAN に対応していないということもある。ここら辺が整理されると、家庭用の IoT 機器が非常に使いやすくなる。業界のルールになるのかは分からないが、現実としてそういうニーズはある。そういうこともこのTFで話ができると幸い。

・ 施設で重要なドアの IC カードのセキュリティについて、IC カードとリーダとの間の通信は相当強固であり破るのはきわめて困難だが、リーダからコントローラやサーバへの通信はとても弱いことがある。これはシステム全体でみると、何のセキュリティにもなっていない。トータルのセキュリティが守られていないケースが結構多く、これを解決していくことも必要。

・ 異業種が集まったとき、言葉の定義が非常に大事である。リスクという言葉の意味も変わってきている。この TF 以外の社会的な動き等もあるので、言葉を合わせていく作業もすれば良いかと思う。

●事務局資料について

・ (資料 4 について)p.11 の台湾のケースは訴訟に発展してもおかしくないように思う。これが日本だったらどうなのか。事業者側がどこまで責任を負うのかはまさにこれから議論という状況。それとの関係で p.30 のリスクをどう考えるのか、というところは興味深い。例えば、プライバシーの問題が発生したときに、プライバシー侵害は、事案によってはきわめて大きな損害につながるケースがある。最近の精神的損害や、刑事責任との関係の位置づけ、さらに、法的な責任とは別に事故が起きた場合のレピュテーションリスクをどこに置くべきなのか等、気になっている。

・ (資料 4 p.26 について)「サイバー空間のデータに基づく制御」の矢印が、「セキュリティに係る攻撃を受けた IoT 機器の意図しない動作」で止まっているところに技術の限界を感じる。意図しない IoT 機器の動作に人間がどう対処するか、というところでフィジカル空間への影響は変わってくる。技術的に何が起こるかは分かるが、起きたときに、どういう影響があるかということは、別の視点の分析が必要。

・ (資料 4 p.30 について)このようにカテゴライズして考えるのは画期的だが、少し安全や影響というイメージが 20 世紀的。例えば、安全といっても、人命や資産という物理的な影響以外にも、経済性の混乱や生活の不便性等、様々ある。そういう面でのマネジメントや、全体的な相互バランスを考えるときの影響範囲も、実態的に社会が使えるところま

で検討すべき。

・ （資料 4 p.30 について）メーカの業種により、生命と財産を守るという言葉の意味が少し違ってきたりする。エアコンや給湯器を作っている会社の方と、Web カメラを作っている方々とでは、それに対する重み付けが若干違ってくる。こういう形でマッピングし、リスクの度合いを表現して、転写という機能の中でも、個人や社会へ影響の度合いが違うということを、うまくカテゴライズして意見が纏まってくると業界としても活用しやすい。

・ （資料 4 p.30 について）この表について、サイバー犯罪としてどこまでカバーすべきで、どこは基本的には民間に任せるべきなのか、という観点や、ある一定の行為が犯罪になるとしてもどの程度の法定刑を以て対応するべきか等に関心がある。関連して、サイバーとフィジカルに加え、社会的影響というようなもう一つの軸もあるようにも思う。

・ （資料 4 p.31 について）赤枠で囲まれた①のところに認証とあるが、セキュリティに関してだけ言うと、100%ではない何かに基づいて評価した結果が、ある時点の、ある基準に対して合格だったということを示すだけである。それに基づくマークがついていたとしても、その後で例えば脆弱性があったということがあり得る。認証という行為が何を意味するのか、消費者、購入者がどう受け止めるかが非常に重要。そういう点について、この TF で考え方の整理が出来れば、分野別 SWG でもアプローチできる可能性があると考える。

・ （資料 4 p.31 について）①は、業界毎に色々な取組をこの場で情報交換できればと思う。業界毎に、進んでいるところとまだ検討しなければいけないところ、でこぼこがある。標準化に関しても然り。全て横並びではなく、しかしできるだけずれない形で議論できるとよい。

●安全とセキュリティについて

・ 安全とセキュリティの両立について、もはや安全とセキュリティの違いを議論している状況ではない。両方をやるしかないので分離することはあり得ない。さらに、IoT の世界では安全とセキュリティの両立だけでは駄目で、実際にものを使う産業のマネジメントも並立させることが必要。安全やセキュリティの観点では課題があっても、社会的には活用せざるを得ないケースはあり、これらが並立していないとこの問題は解決できない。

・ 本質安全、すなわちリスク源を断つという考えがあるが、IoT 機器は、機器やネットワーク自体がリスク源なので本質安全が使えない。今までの安全問題からすると、全く異なる状況が起こっている。そういう意味では、アプローチ方法も含め、今までの技術の中の組み合わせだけではなく新たな枠組みを作らないと意味がない。

・ 資料 4 の p.26 にある上の矢印と下の矢印の信頼性と安全性をどう担保するか、が本 TF のアウトプットになるだろう。セーフティの方では、リスクアセスメントに始まり、リスクアセスメントに終わるという形で危険の事象の管理をしているので、それに関連してセキュリティリスクという考え方は当然必要である。セキュリティ・リスクアセスメントと、セーフティ・リスクアセスメントを同時に両輪として行っていくことによって、各個人であれ社会であれ、リスクを最低限に低減させるための方策をまとめることができればよい。

・ セキュリティとセーフティを含めて、全体のガイドラインが必要。しかし、全体からみると、相当広範囲に亘るので、どのような形でまとめるのか考えないと、あまりにも技術的に深い話ばかりやっていると、時間との関係で全体の話がまとまらない。そこの両方を、どのようにマッチングさせて時間内に納めるのかというアプローチを考える必要がある。

●分野別トピック

- 最近では医療機器でもスマートフォン等を使っており、医療器なのか、非医療器なのか、意図する使用（Intended use）を明確にすることが重要である。これまで日本では、どちらかというと病院がセキュアな環境を作っていることが多く、医療機器製造販売業者と医療機関の連携不足もあり、情報共有も含めて曖昧な点が多かった。厚労省のサイバーセキュリティ関連の通知では、この辺 Shared responsibility ということで明記されている。医療機器がネットワークに繋がると、攻撃によって大きな事故を引き起こす可能性すらある。FDA のガイダンス等、医療機器におけるサイバーセキュリティに係る規格などでは、ネットワーク化によりリスクマネジメントの考えとして、「フィジカル」という表現を削除して改訂されている。

- スマートホームSWG において、スマートホームとは何か、ガイドラインの中でどう扱うのかという議論を始めたところ。今後、ユースケースを立てて、どういったリスクがあり、どういう対策をしていくか、という議論を今後深めていく予定。また将来的にガイドラインが出来たとして、そのガイドラインをどう活用していくかというところが非常に重要になってくると思っている。セキュリティに関して、認証とは何か、何を意味するのか、という考え方の整理がこの TF で出来れば、スマートホーム SWG でもアプローチできる可能性があると考える。

- これまで電力 SWG において、オリ・パラリンピックも見据えた短期的な対策として、今出来ること、早期に出来ることを検討してガイドラインに反映するよう対応してきた。現在は、中長期な観点で、大きな課題の一つであるであるサプライチェーンリスクへの対応等について検討している。

- サイバー空間からフィジカル空間への影響が大きくなってくると、人命に関わるケースも出てくることが予想され、どうしてもメーカ側が責任を問われるケースも増えてくると考えられる。一方で、現時点では保険はサイバー攻撃による物理的な損害の発生を想定しておらず、適切な免責の規定などの対応が不十分。グローバルでは動きが始まっていて、免責にするケースだけでなく、広く対応する代わりに保険料を多くもらうケースやサブリミットといって限定額しか払わないというようなケースなどある。フィジカル空間のセキュリティ対策を検討する一方で、適切な保険を提供することでのリスクの移転についても重要であるので、整理していく必要があると考えている。

- 学術会議で工学システムの社会安全目標を議論していたとき、工学システムにも非常に多くのパターンがあり、初めはそれを包括的にやろうとしたが無理があって、カテゴライズしてカテゴリ毎に安全目標のパターンを作った。色々なものを全て一括で議論するのは、具体的になればなるほど難しい。共通の要素で議論できるところと、対象によって議論を分けるというような体系化を、まずやってはどうか。

●TF の今後の方向性について

- 資料 4 の p.31 の図において、左側に各 SWG があり、業界・分野毎に活動されている。これをどのような統一的な観点で考えれば良いか、ということがまず必要だが、分野の特性があるので現実にはなかなか難しい。p.30 のようにカテゴライズをしたとして、それぞれ毎に観点が違ってくるだろう。期待は非常に大きい。

- 標準化を目指すのであれば、多くのTCがある中で、どこにどうやってアプローチするのかを時間をかけて絞り込んでいけば良い。CPSF は、ビジネスモデルを描くことができかなり良いモデルなので、どのように使っていくか議論できるとよい。

- 事務局への注文だが、このように技術進展の早いものを議論するときに、事故事例を踏まえて議論する、というやり方は難しい。議論のやり方も含めてご検討頂ければ幸い。リスクを網羅することは不可能であり、あらゆるものをやる必要はなく体系的、論理的にやれば良い。大事なのは、例えば 2 年かけて議論するとしたときに、この議論の結果が活用される社会がどのレベルかということを押さえておくこと。2 年あれば色々なことが出てくる可能性がある。その技術の進展ということも、ある程度目途をつけて議論しておかないと、2 年後に 2 年前の世界で議論していることにならないかという問題提起。

- 近年、製品の脆弱性を狙った攻撃やインシデントが増加しているが、IoT 機器自体や制御機能自体をターゲットとするものではなく、転写部分を経由した、いわゆる踏み台的な使われ方が多い状態。脆弱性を悪用した攻撃があった場合、脆弱性の解消を目指すことになるが、コスト負担の問題など、製造メーカ、販売代理店、運用保守しているメーカ等の関係者の利害関係が衝突し調整が難しい。この TF のような場を通じて、各関係者が行うべきことなどを整理して、関係者が無用な衝突をせずに済む共通理解のようなものが示されるとよい。

- SWG が業界毎にあるなかで、本 TF では横串として、消費者に提供できるような最低限の条件をここで議論できるのが良い。認証等もテーマの一つと思う。最小限の認証は、業界を跨いでもこの程度だろうという話だったり、全体的な評価をするときのフレームワークだったり。業界毎にルールがバラバラで、消費者が困るというケースを解消できるようなことが出来ると良い。

以上

お問合せ先

商務情報政策局　サイバーセキュリティ課

電話：03-3501-1253