# 産業サイバーセキュリティ研究会
# ワーキンググループ3(サイバーセキュリティビジネス化)(第3回) 議事要旨

## 1. 日時・場所

日時:平成31年1月28日(月) 15時00分～17時00分

場所:経済産業省 本館17階東8 第2、3共用会議室

## 2. 出席者

委員 :國領委員(座長)、東委員、飯島委員(代理:吉田様)、石井委員、石原委員(代理:教学様)、稲垣委員、鵜飼委員、鴨田委員、栗原委員(欠席)、篠田委員(欠席)、手塚委員、花見委員、古田委員、宮澤委員、三輪委員(代理:村上様)、本島委員、山内委員

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、外務省、独立行政法人情報処理推進機構、一般財団法人日本情報経済社会推進協会、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:商務情報政策局 西山局長、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、奥家サイバーセキュリティ課長、土屋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 委員等名簿

資料3 事務局説明資料

## 4. 議事内容

國領座長が議事を進行した。

最初に、資料の確認と委員の出欠状況について事務局から説明。

- 資料は 3 つ、議事次第・配布資料一覧、委員等名簿、事務局説明資料。参考資料として、現在パブリックコメントをしている「サイバー・フィジカル・セキュリティ対策フレームワーク(案)」。
- 本 WG の委員は、資料 2 の通り。飯島委員の代理として吉田様、三輪委員の代理として村上様、石原委員の代理として教学様に出席を頂いている。また、本日は栗原委員が所要のため欠席、篠田委員が体調不良のため欠席との連絡を受けている。

次に、本日の議題に入り、事務局より資料3の説明があった。

資料説明の後、以下のとおり自由討議を行った。

(1) 全体について

- 内閣府で動いているスーパーシティや、国土交通省でやられているスマートシティの議論の中で、街をDX化するかという動きが出てきている。その際には、当然ながらセキュリティの文脈がある。都市空間のDXの文脈で、どういうセキュリティのバランスが良いのか歩調合せが大事。都市のDX、デジタル化というところのアーキテクチャ作りに今回の検討内容が生きてくると思う。次のステージのエコシステムを作るのであれば、総務省や国交省、色々な企業も含めた議論を開始するよいタイミング。都市空間のDX化では、地方によってモデルが違うし、また、恐らく重要インフラの中でも交通と医療の繋がりや、エネルギーと交通の繋がり等分野ごとの連携という話が出てくる。そのと

きのファイナンス、ソーシャルインパクト・ボンドや情報の信託、そこに絡んでいる自治体の社会保障等を一体的にデザインしないと面的な広がりはなかろうと思う。

- 都市のDX化の本質はお金の流れが変わることと思っている。ただし、普通の土地開発という文脈で捉えると、取り違える。エネルギーの分離も行い、これからは軌道系路線の赤字、不採算路線をどうするかという話もあるので、民間も公共も投資の流れが一気に変わるため、民間だけではなくパブリックが最初から入ってくるという点が重要。
- セキュリティに関する知見や取り組みを制度化して、産業化し、資金を流し、活性化して社会に定着させるためには、ユーザーが資金を出すメカニズムの上に乗ることが必要。買う側の動機形成や資金を出す時の決断、経営環境、価値の流通に検討課題が向けられていない。ユーザーが知りたいのは、どれ程できるかではなく、どれ程できないのかということ、あるいは、どれ程できない可能性があるのか分からないのかということ。例えば、検証基盤の問題については、リスクアセスメント方法の論理性や合理性、取り組み時の資料収集の適切さと等、いくら評価しても興味がどんどん動いていくので、分からないので、どれほど分からないのか、あるいはどれほどいい加減ということも評価できるような仕組みにする必要がある。
- 評価することは評価者に対する責任問題にも繋がるので難しい問題だが、やってみたら動くこともあるので、とにかく挑戦することが一番重要。ハッカーを認定するという仕組みも、不完全さを許容して実際に進めることを優先し、動かしていく中で生じる問題に対処していく必要がある。日本独自の仕組みを生み出すためには、リスクを許容して挑戦する必要がある。ビジネスが育つ環境を作っていくという目標の下で、チャレンジすることを念頭に置きながら、色々な政策を進めていって欲しい。

(2) サイバーセキュリティ検証基盤の構築について

- IPAのICSCoEと連携のアイデアが出ているが、特に製品選定のポイントなど、この環境を使わない手はないのでないのか。産業育成の観点では、例えばあるベンチャーの技術の評価に関して一つのカリキュラムとし、新しい技術の応用等を議論するなど連携に関して考えていただきたい。
- 複数の視点が、混ざっているような気がする。プロダクト、セキュリティ製品自体の機能の良し悪しの話と、いわゆる製品のセキュリティ品質が高いか低いかという話は別の話で違和感がある。
- 誰が評価をするかというところが非常に重要。セキュリティ製品を評価するには、例えばマルウェア対策製品であれば逐一防御できるというところは重要だが、運用性、使い勝手、サポート体制、経営基盤等、色々な視点が必要。有識者も、色々な立場の人達をうまく入れて評価できる仕組みを作らないと、実質的にユーザーで使っていくという視点と評価が結び付かない可能性がある。
- 今回のような取り組みを進めていく中で、ウェブサイトに有識者による評価を公開してくという話だが、ベンダーからするときちんと評価をしてもらえず、誤解を受けたまま酷評される場合もあるので、ベンダーが主張できる場を作って欲しい。また、ベンダーが納得できない場合は、掲載を降りられる仕組みを作っていただけるとありがたい。また、この手のランドスケープに作ると、たまに、有象無象で怪しげな人たちもいるので、その点は、有識者を交えて議論した方が良い。
- 製品評価については、形骸化した評価にならないようにする事が肝要である。例えば、広く知られた評価としてIPAの「情報セキュリティ10大脅威」というものがあるが、これは選別されていない不特定多数のセキュリティベンダー業者によるアンケート形式の為、各セキュリティベンダーが売り込みたいセキュリティ機器に関する脅威が選出される傾向がある。本WGで検討しているセキュリティ製品の性能評価でも同じ事が起きぬように、評価者は精査して選別する必要がある。具体的には、サイバーセキュリティの有識者や大学教授だけではなく、サイバーセキュリティの機器を日頃から触り製品の性能及び動向をよく知っているユーザー企業に参画して頂く事が重要であり必須であると考える。
- 検証基盤の構築について、難しいかもしれないが、導入した企業、もしくは匿名でも良いので、実施内容などの導

入実績の公表は進めて頂きたい。各セクター、国なども含めて、この様な取り組みをもう少し進めて欲しい。

- 導入事例も、是非検討いただきたい。経済産業省等が利用しているセキュリティ製品等も、もしあれば、率先して公表していただけるとありがたい。
- 評価の問題は時間軸からすると1番後ろの方でも良いと思う。評価となると第三者評価、あるいは有識者となるが、本当にユーザーが有識者の第三者評価を求めるのか、また、どれぐらいのこの価値転嫁ができるのか等の問題意識もある。是非この辺は他の制度がある程度動き始めて、ユーザーにその価格転嫁の道が見えるような段階になってきた段階で、進めていただくのが効率的である。
- この検証体制には、金融が入っているが、金融のテクニカルなものを知っている人達をどんどん入れていくべき。
- Checked by Japanというキャッチフレーズを付けられたのは非常に良いことだと思う。海外に向けメッセージだと思うので、日本は本当にこういったサイバーセキュリティ製品に対してチェックができるのかという海外からの目を意識しないといけない。日本人はどちらかというと性善説で、悪が少ない。攻撃者の立場に立って多様な攻撃への対応も想定した対処ができているかも含めたチェックをしないと、セキュリティ製品のチェックができたとは言えない。
- Checked by Japanを、日本独自の考え方で、日本から発信し、ビジネスも含めて日本がイニシアチブを取っていくということが一番重要だと思う。
- 評価の判定を下すことは急ぐ必要はないが、評価方法は拘るべき。資料3の4ページの図の中で特に赤の部分の検証方法というのは、まだこれからやるべきことが多くある。ここは積極的に研究開発投資、公的支援をして、日本独自の方法を生み出し、それがChecked by Japanというブランド確立に繋がる流れにすべきだと思う。
- 現在のセキュリティ製品はクラウド環境における動作を対象としたものが多く、また適用されている技術の多くはAIやマシーンラーニング技術を使っている。これらの技術を適用した製品は、攻撃情報の学習を通じて検出力を向上させていくことを前提としているため、出荷時期だけでは製品や品質を特定できない。品質評価には新たなアプローチが必要である。例えばAIで注目されている敵対強化学習においては、お互いの学習結果をぶつけてAI自身が能力を向上させていくような自己学習強化メカニズムがあるが、こうした新しい技術を活用してセキュリティ製品の評価を自動化するツールを日本で開発して、それが、資料3の4ページにある青（実環境における試行検証）と緑（セキュリティ製品の有効性検証）と赤（ホワイトハッカーの実攻撃検証）につながるような、これらを有機的に結び付けていく発想があって欲しい。
- 海外からの認知を高めるためには、現存する国際基準、フレームワークとの関係を明示することが重要。サイバー・フィジカル・セキュリティ対策フレームワークにおける対策要件CPSの中で色々謳われている要件が、例えば製品検証のどれに関連付ける等、今進めている取り込みと紐付けていくというのは非常に大事。
- サイバーセキュリティの検証基盤だが、国際的に見るとヨーロッパ系の認証の仕掛けはしっかりして、Common Criteria系から来ている世界があり、機能を検証することで保証要件がどうなっているかという保険の評価だと思う。そのときに基準をどう設けるかということが重要で、そこをしっかり作る必要がある。基本的には、実際に評価するのは官民問わず認証された人達が行えば良く、第三者機関をしっかり作って回していくという考え方だと思う。
- 資料3の8ページと10ページに、それぞれ海外の有効性評価に関連する事例という同じような形で出されているが、その方向感が違うものだと感じている。10ページにあるような、正しくカタログ通りに動作することやセキュリティ製品としては当然備えておくべきスペックに対して確認する評価と、8ページにあるような、マーケット全体を見渡した時に、面白い取り組み方・やり方、あるいはチャレンジの仕方を有識者が評価する評価というのは、違う話かと思っている。産業セキュリティということであれば、今後、攻撃方法や、守っていく方法も新しくなっていく世界なので、この8ページにあるような、面白い考え方、チャレンジの仕方、あるいはそれにチャレンジする人や団体をピックアップするような取り組みというものを、取り入れて頂きたい。また、そういった方々が実際にビジネスを広げ、大きくなっていくにあたって、色々な評価を経て、より強固な問題のない、あるいは多くの用途に対応できるような製品作りや体制作りができるような仕組みが、10ページのような形を通してできるのが理想。是非分けて考えて、両方を見ていた

だけるとありがたい。

- セキュリティの基盤は、それはエコシステムなので、製品単体というよりは、むしろ繋がった形でどう評価するかということを考えなければいけない。
- エコシステムとしてのビジネス活性化に当たって、検証基盤や認定制度が、1つ大きなプラットホームにと思う。その点では、資料3の4ページの緑や青のような評価で、例えばICSCoEやCSSCを活用するというのは、1つ手段かもしれない。ベンダー、メーカーに偏る訳ではなく、ある一定の公平さを持って評価できる場所としては良いのではないかと思う。一方で、資料3の4ページの赤の方（制御系システムの評価）は、制御系システムでは、未だメーカーもばらばらで、実際の現場では色々なシステムの組み方をしていたりするので、ICSCoE等の評価で大丈夫というような甘い世界ではない。信頼認定された検証主体が、ホワイトハッカーを含むものと捉えているが、複数生まれてくることが、まずビジネスの活性化だと思う。認められた機関が複数あって、それらが現地に赴いて、しっかり検証する環境を作ることが、依頼する側の安心感であったり、お墨付きであったりという感覚になる。ただし、実際これを回していこうとすると難しい。技術も進歩するし、インシデントが進化したり、新たな知見が加わったり、規格もアップデートされる。こういったものに常に追従している機関であるということを認定する仕組みが必要。検証主体になり得る実力のあるところであれば、例えばベンチャー企業であっても、非常に尖った実力を持っていれば、例えば、大企業のシステムに一気に入りやすい環境が作れるのではないかと思う。
- 全部できあがったシステムの評価を、どうやるのかを考えていかなければいけない。ここがしっかりできれば世界に冠たる日本のセキュリティということで、様々な輸出産業にもリンクできるのではないか。
- 下からの積み上げでシステムを見るのは、相当な至難の技で、すべてのケースを対象にすることはできない。セキュリティバイデザインがあるとして、セキュリティバイデザインを手がけられる人は誰かと考えると、建築だと1級建築士等の考え方があり、その人達が信頼の下でやっている。システム構築の時に、そのセキュリティバイデザインを担える人は、どういう人なのだろうか、まず、そこに一度トラストアンカーを置いてみたらどうかと思った。このような仕掛けを日本で世界に先駆けてやって、それでシステム構築などの時にお墨付き的な部分を担えるような仕掛けを日本の中で少し回してみることは、やってみる価値あるかなと思っている。
- 今のケースは経産省が、システム開発のモデル契約書作っていて、その中でもうすでに謳われている。制度としては、セキュリティ監査とかシステム監査にも入れている。問題は、ふさわしい能力があるかということ。それを鍛えていくってことは大事だが、枠組みとしたら、もうすでに経産省が考えていること訳で、是非充実させていって頂ければと思う。
- ユーザー企業としては、早くこういったものができるとありがたい。特に、赤のホワイトハッカーの実攻撃検証等。当社の製品もIoT機器の1つになるので、攻撃の検証を進めている。ただし、できる人が日本に非常に少ない。万一、脆弱性が見つかった時に、それを他の国に持っていかれて、対応を完了するまでの間、非常に不安な日々を過ごさざるを得ないこととなる。自動車のセキュリティは、セキュリティの中で非常にニッチなところなので、自動車向きにこういった仕組みができると思わないが、是非、一緒に作らせていただきたいと思っている。
- 今回重要だと思ったのは、出口戦略として、検証評価をどうやってうまく回して、ビジネスに繋げていくかという、そのフェーズ。ビジネスとなるとやはり実際のフィールドでワークしている世界で、そこにフィットした対象として検証する考え方をどう整理するかというのが、非常に日本にとって重要。
- 協調領域と競争領域を分ける必要がある。競争領域的なのが入ってくると、やはり自社のものを売り込みたいとか違う角度の要素が入ってきてしまう。そういうものをうまく切り分けて協調領域というところでその出口戦略に持っていくのかが重要。その辺を日本ならではの手法が見出だせると、これは世界に持っていけるのかなという思いを持っている。どうやって評価していくかというところをもう1つ深めると、非常に高い価値が生まれてくるのかなという気がしている。
- 今日の資料等にはないが、いくらシステムを強化してもいくらツールを導入しても、やはり使いこなす人がどこまで

実力を持っているか、という評価軸が非常に大事。運用する力を評価することを考えていきたい。人、また組織に視点を当てることを、ビジネスの活性化という視点で考えられないかなと思う。

(3) サイバーセキュリティお助け隊について

- お助け隊について、中小企業のセキュリティ意識を高めるには、やはり国等の大きな力が、後押ししていただけることが非常に大きいと思っている。中小企業のセキュリティは、難しいマーケット。手強いお客様なので、この旗振りが、現場の中小企業にうまく機能するか、色々な課題も出てくると思う。課題が見えたということも、1つ大きな成果。
- 中小企業のセキュリティには、いくつかフェーズがあると思う。既に攻撃されてしまったことに本人が気づいた場合は、お助け隊で相談ができると思うが、攻撃されているのに気づいていない人達や、あるいは、たまたま攻撃されていないだけで、脆弱性や穴があるまま運営していく中小企業など色々ある。攻撃されているのに気付づいてない人達に気付かせることが重要。何らかの監視サービス、あるいは、警察等の捜査機関等では、中小企業を踏み台にしてどこかがやられたときに、元々踏み台にされた場所を把握できる手段はあると思う。そういった捜査機関等とも連携することによって、早く対処しなければいけないと気付づかせ、お助け隊をうまく活用していく運用ができるのではないか。
- 事業としては難しい面もあると思っている。ひっきりなしにお悩み相談が来れば良いが、人を抱えたものの、お悩み相談がないとそのコストをどうするのかという課題がある。最近セキュリティ女子という言葉も出てきているが、産休や育休の方、家でも出来る仕事がしたいという方をうまく活用するのも一案だと思う。
- 資料3の19ページの図は、どちらかというと中小企業のOAをイメージして描かれているようだが、都市であったり地域だったりということを考えた場合は、レイヤーを分けて、例えば、一番下にベースとしてIDS等をNFVでキャリアが持って、非常にライトウェイトな形でネットワークレベルでの問題を早めに発見する、その上に保険と絡めたような形があり、更にその上にOAのプロトコルといったようなところの対策といった物が重なるマルチレイヤーの取り組みでサポートしてくような仕組みが必要なのではないかと思う。
- 多くの中小企業にはITの専門家が居るわけでもなく、何がリスクなのか分からない状態。こういった人たちに難しいことを言っても、理解を得ることは難しい。できれば生命保険に入るときの健康診断のように、点検項目をチェックするだけで良く、万が一のリスクは保険でカバーできるという形でサービスを提供しないと進まない。生命保険に入るのに医学的な知識が不要であるように、サイバーセキュリティも健康診断に相当する状況把握方法が必要ではないか。
- サイバーセキュリティお助け隊については、経営者の意識改革を進めるためにも、サポート機能を明確化して、支援内容や危機を明確にした方が良い。また、クラウドサービスを使っているケースも当然あるので、オンプレミスとの組み合わせでの支援内容も検討した方が良い。

(4) 情報セキュリティサービス審査登録制度について

- セキュリティサービス審査登録制度については、公的に活用されれば、ユーザーの役に立つと思うが、制度が乱立すると分かりにくくなる。似たような制度を乱立させないで、お助け隊と連携させる等、使いやすい環境を作って頂きたい。

(5) コラボレーション・プラットフォームについて

- 我々民間も、学と一緒にコラボするというところについては、非常に魅力を感じている。ただし、どんな大学がどういう研究をして、どういう強みがあるのかというのは、なかなか見えていない。体系的な情報があると、ドアノックしやすい。学と民が組むことに、色々なメリットがあると思うので、民間側がもう少し積極的に使えないか考えている。

(6) 委託時の責任範囲の明確化について

- 委託範囲に関する責任問題については、一定の考え方に基づいて先行して取り組みを進めていっていただきたい。基準を作るにしても人材育成にしても今後社会制度として定着させるためには契約が必要になる。しかも今後の社会制度を適用する社会は、ネットワーク化された非常に広範なサプライチェーンを一括して捉えて、そこにおける自分の位置を把握しながらリスク情報を提供する、相手とリスクを共有するといった判断をしながら社会を安全にしていくということ。そうすると、どうしても責任範囲の問題が、あらゆる場面で出てくる。先行して進めていただきたい。
- 絶対に必要だと経験的に思う視点は、責任原理。今までの近代法的な責任原理をいきなり否定する訳には行かないが、それに囚われない方法は何か、それを修正する方は何かという観点の捉え方を是非してもらいたい。具体的には、事象を解決する、その後で責任を考える、あるいは資金が動く、その後で適正化するという手法が、是正的なものだと思う。その方法を考えていかないと近代的な責任原理を乗り越えられない。
- 近代の考え方では、意志が絶対に尊重されなければならない。従って、原因は誰が作ったのかということがはっきりしない限り責任を負わないとか、あるいは過失がない限り責任を負わないという原理になってしまう。そうすると、これらが解明されない限り責任を負えないということになる。この社会を前提とした枠組みがすでにできている。ところが、サイバーフィジカルネットワークとか、コネクテッドインダストリーの想定する社会は、そういう社会構造ではなく、インターネットのように分からないところで一定の機能を果たす、そして社会全体を機能させるという構造になってきている。できれば近代法的な法廷法的原理を否定してほしい。そこまで行かなくても、それを修正するような、まずは資産が動く、資金が動く、責任は後から追及すると、いう様なところに行かないといけない。是非そういう観点で、まず資金なり、事象を動かすための資金の流れの仕組みを作っていくべき。
- 参考になるのは、ソーシャルインパクト・ボンドや、例えば役所の仕組み。何が起こるか分からないけど予算を付けて動かしてみて、その中で良いものに実現してく。それから保険業界の方でもSRI、社会的責任投資の問題とか様々な取り組みがなされていると思う。保険も通常の保険を考えると保険数理に基づいて責任原則に基づいた保険ということになってしまうので、そうではなくて、むしろ先程の社会的な課題と取り組むための保険原理、あるいは信託制度の検討を是非進めていっていただけたらと思う。先進的に、世界に先進的に進めてもらいたいと思う。
- 責任の範囲のところについては、保険があると、そういったところがうまく守れるというのは、我々のインフラとして機能できるところが多分にある。
- 今回の責任関係の調査というところは、ITの受注発注の関係に基づく委託のところが中心であって、一番分かりやすく、大元のところであると思うが、サプライチェーンの関係で行くと、発注先・発注元のシステムに伴わない取引先と取引元の責任関係は、もっと曖昧でグレー。サプライチェーンを支える元と下請けとした発注先等の責任関係に、メスを入れていけるような状況になってくれば、混沌とするかもしれないが、良いのではないか。
- 責任の問題は、考えれば考えるほど難しい。例えば、評価に関しても、製品を評価する、誰が評価するかということで責任が付きまとう。人数が多ければ良いかというのも難しい。突き詰めれば突き詰めるほど、課題がある。ただし、評価する人自身には責任を持たせたら駄目なのではないかと思っている。
- 今のサイバーフィジカルネットワークが想定している社会は、近代的な責任原理では成立しないところ。事実と責任ではなくて、リスクと投機、これをベースに社会の仕組みを作っていけば、ユーザーの感覚に合う。ユーザーは分からないものに金を出す。リスク全体社会と言われてもう15年ぐらいたつ訳だから、むしろ事実ではなくてリスクに金を出す、投資をして回収できる、そういう仕組みを考えていける検証事業や検証仕組み、評価の仕組みをやらないと、形骸化した評価制度、検証制度、責任だけのものになってしまう。検討対象や検討体制を広げて頂きたい。

(7) その他

- 配布されたサイバー・フィジカル・セキュリティ対策フレームワークで、NISTのフレームワークのSP800-171等との参

照があるが、非常によい試みだと思う。今やっているような取り組みが、唯我独尊でやっているというように捉われては、なかなか海外からも認知されない。NISTのフレームワークと関連付け等は、認知されてく枠組みになる。

最後に、西山局長から以下の通り挨拶。

- 先週安倍総理がダボスで演説をされて、その1つのコンセプトとして、データ・フリー・フロー・ウィズ・トラストと言われた。ウィズ・トラストのトラストとは何か、もう少し因数分解が必要。勿論、今までの社会でも、トラストを確保する仕組みがあり、社会が成立していたが、Society 5.0になると、トラストを確保する仕組みが変わる。
- そのトラストをどうやって確保するかということを我々は、非常も広い意味でガバナンスのイノベーションだと言っている。それは当然プライバシーの世界でもあるし、広い意味でのフィジカルな安全性の世界でもあるし、普通に取引が成立するという意味でのトラストもあると思う。
- 我々にもまだ今具体的なイメージはないが、それらは恐らくお互いに繋がっている。サイバーセキュリティだけのトラストがあったり、取引を成立させるだけのトラストがあったり、プライバシーだけのためのトラストがある訳ではなく、それ自身も繋がっているということなのではと思っている。
- 今日ご議論いただいたような話も含めて、そのトラストを確保するための、今まで異なる、しかも分野ごとには関係しているガバナンスの仕組みを作る工夫が必要であるため、それを日本から積極的に発信をして、チャレンジをしたいと思っている。このワーキンググループでも、引き続き活発な議論を続けていただき、是非日本から、発信もしていきたいと思っている。

**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