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4回) 議事要旨

1. 日時・場所

日時:令和元年8月2日(金) 15時00分～17時00分

場所:経済産業省 別館11階1107共用会議室

2. 出席者

委員 :國領委員(座長)、東委員(欠席)、飯島委員、石井委員(代理:岡田様)、石原委員、稲垣委員、鵜飼委員、北山委員、栗原委員、篠田委員、手塚委員、花見委員、古田委員、本城委員、宮澤委員、三輪委員(欠席)、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、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 委員等名簿

資料3 事務局説明資料

4. 議事内容

冒頭、西山局長から以下のとおり挨拶。

- 6月にG20を主催し、データ・フリーフロー・ウィズトラスト等の新しいコンセプトを打ち出した。世界で利害が対立する中で、我々が思っている以上に日本からコンセプト、ルールを提案することについて、諸外国の期待が非常に高い。
- コンセプトを発信するだけではなく、日本の産業の裾野、ビジネスの強化につながらないといけないと思っている。本日も是非、皆様に積極的に御議論頂いて、コンセプトのみならず、産業、ビジネスの面でも世界をリードできるようなものにしていきたいと思っている。どうぞよろしくお願い致します。

以降、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、議事次第・配布資料一覧、委員等名簿、事務局説明資料。
- 本 WG の委員は、資料2の通り。今回、人事異動等に伴って委員の変更があった。鴨田様に代わって本城委員、本島様に代わって北山委員に参加頂くことになった。
- 本日は、栗原委員は、所用により遅れて出席、石井委員の代理として岡田様に出席を頂いている。また、東委員と三輪委員が所用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

- WG1 ではフレームワークを作ってきたが、産業サイバーの視点がやはり強い。もっと生活者視点でいろいろ考えてみたらどうだろうか。
- 資料3の2ページのところで、大分ストーリーラインを密に作ってきているなと感じている。全体的なフレームワークが、今回見えてきたという点で前進であり、すばらしいなと思っている。
- AIがいろいろなところで問題になっている。AIは学習してルールを作るが、悪意のあるデータだと、結局ルールが悪意を持ってくる。そこをどう評価するのかが、重要になってくる。そのような領域等、いろいろとあると思うので、少し幅広で考えて頂けたら良いと思う。
- IoTの先にあるのは、情報流通や情報マーケット等が出てくる。情報を安全に利活用する事が必須になってくるが、情報をモノと同じように売り買いする様な対応でいいのか、社内でも議論していて、特有のガイドラインがあった方が良いのではと思っている。この会議体で議論するのが良いかは分からないが、そのようなことも、意識しながら進めるのが良いのではないか。

（2）Proven in Japan（検証基盤）について

- ベンダとユーザのお互いに、公表するメリットがある世界を作っていくことが重要。ベンダ側は、ユーザ個別の社名を出さないのであれば、実績を公表しても良いのではないか。ユーザ側には、公表することで、対外的な信用を得ていくとか、保険の優遇等があると良いと思う。
- 海外企業の事例では、事故や脆弱性があった場合に、ベンダがそれについてきちんと対策をしたということを繰り返し流していて（世の中に訴えていて）、それが逆に信頼を生むということがある。日本は、公表することに対してベンダがユーザに配慮するために積極的な状況ではないと考えるあまり積極的に出していないことによって、世間の信頼を得られていない側面もある。
- 事例の公表は、双方にインセンティブがあるから行っており、例えば、ベンダ側は、事例を公表させてくれるならば値段を下げる、というようなことを対ユーザでやっている。また、海外であれば、民だけでなく官についても、例えばアメリカ国防総省などが事例を出している。官と民では、それぞれ事例公表を後押しするためのインセンティブも違うと思うので、そのような官による事例公表に関する検討も併せて行って頂ければと思っている。
- 実績公表は、少ないから目立つが、多くなってくれば、自分のところもやらなくてはいけないとなるので、増えてくると思う。増えてくれば、宣伝にもなる。事例を公表させてくれた企業に花を持たせるという意味で、地方の記事に載せる等、プロモーションを考えたら如何か。
- 資料3の4ページの緑、青のところは、有識者が一方的に製品・サービスを評価するのではなく、有識者とベンダの間でいろいろと意見交換等ができる場があった方がフェアだと思う。
- 赤の海外との連携のところで、海外企業に一番美味しいところがもっていかれるような状況にならないように、注視をしていく必要がある。例えば、各会社は、人海戦術的に脆弱性を探していくようなホワイトハッキングのようなノウハウをいろいろ持っているが、それらをツール化して、販売していくツールベンダが海外におり、利益はどちらが大きいかというと後者の方が大きい。
- Proven in Japanや審査登録制度は、事前チェック型だが、実際システムが動いているときのランタイム時のチェックで、安全な環境、安心安全なサービスが実現されていくのも、もう一つの側面。その両面が出てくれば、最初の導入の前提的な動きは、大分見えてきたなという気がしている。
- 緑青の評価については、コストとライフサイクルのバランスを少し考えた方が良いかと思う。例えば、ICカード、ECSEC等では、ライフサイクルが10年ぐらいあるので、ハード、ソフト含めて評価可能だろうが、ライフサイクルが短いものだと、3ヶ月、半年かけて評価すると負荷が大きい。評価は、どこの時点で何をするのか、それを毎年やるのか、一定の期間ごとにやるのかを考えて頂けたらと思う。
- 資料3の5ページの重要分野予測というところだが、重要分野の市場での時間軸は、大事な話。重要の意味合いも、

まだ対策がとられておらずこれからやらなくてはいけないから重要等、いろいろあり得る。重要というところの意味合いについては、もう少し議論してもよいのではと思う。ポスト量子暗号のような話も、視野に入ってきておかしくないと思うし、AIを用いた予測システムが当初想定してしない誤動作を引き起こすといった新たなタイプの脆弱性等も当然サイバーセキュリティの分野に入ってくる。また機能面からは、未知の攻撃に対しても、どこまで対処可能かといった汎用性の観点等、いろいろと評価軸がある。

- 重要分野とあるのは、セキュリティの分野というよりも、どういうビジネスであるかとか、どういう問題が発生するから、こういう領域が重要になるということだと思う。何処が重要になってくるかを捉えて、見極めるのが重要かと思っている。是非、そこを考えて欲しい。
- いまだに、認証ビジネスが成熟していない中で、認証に対する責任を誰が取るのか、確実に中立性を持って認証をやるにはどうしたら良いのか、人に依存していると継続性が無いので、組織としてやることが必要なのではないか、と考える。認証の更新サイクル等、ISOと同様な考えになるのかも知れないが、やはり、認証を本気でやるのであれば、どうするかというのを、考えないといけないと思う。
- イスラエルにしろ、アメリカにしろ、何故これだけ競争力があるかというと、思うに、彼らはサイバー戦争で命を懸けて対処技術を向上させてきており、そういう技術開発経験のある人達が、自分で商売をしているから。日本は、そういう緊張感が経験できる場がほとんど無いので、ゼロからやるのは難しいと思う。情報技術は、積み重ねの技術なので、ある部分までは現時点で活用できる技術の適応を前提として、その土台の上に日本製品の競争力強化につながる差別化できるものをどのように創り出して行くかを考えなければいけない。
- 時間感覚が重要。働く環境等が、大分変わってきている。ほとんどクラウドがインフラになりつつあるというお客が増えてきた。働き方が変わったところにおけるセキュリティは何か、少し考えていく必要がある。
- 検証基盤の取組を通じて得られる情報を、例えば、日本のセキュリティベンダの特許戦略とか、世界に対する勝ち目を付けられるようなところに利用できるような仕組みにしてもらいたい。
- IoT 分野では、プロトコルも千差万別数多く存在するので、プロトコルを前提としたセキュリティ対策は、分散化するリスクがある。多様なIoTプロトコルのアナライザを国の方で整備、提供し、各社はそれを活用した製品を独自に開発していくといったことが考えられる。セキュリティ製品の競争力強化に資する共通基盤整備を公的にどのように支援していくか、議論していくのは良いのではないか。
- IoTでも、プラットフォームを含めてシステムになっている。どこからどこまでを検証する必要があるか、デバイスもどこまでか、というのも重要になってくる気がしている。その辺りは、議論を深めていった方が良いかと思う。
- 資料3の9ページの有識者の評価で、対象となる製品・サービスの箇所で、製品という意味では大変わかりやすいと思うが、サービスは、いろいろなものを組み入れるようなものもあるので、対象を明確にする必要があるのではないか。

(3) 情報セキュリティサービス審査登録制度について

- 審査登録制度について、弊社としては積極的に活用しようと思っている。さらに、グループ企業も、地方の企業だと訴求できる場が限られているので、積極的に活用していきたいと思っている。
- 登録料が必要なので、もし、審査登録制度に権威を持たせていくのであれば、Proven in Japan(検証基盤)との違いを整理して欲しい。サービスを登録する側からすると、両方やることにインセンティブがあるのか気になるところ。
- Proven in Japan のペネトレーションテスト事業者を審査登録制度で評価、審査するのは、賛成。
- 審査登録制度は、先程から言われているようにインセンティブというところが肝要で、ユーザが集まったらベンダが集まってくる。ユーザが参加したがる仕組みを作らないといけないが、そもそも地方、中小企業にはセキュリティを入れないといけないのか、と考えている人達も多いので、そこからだと思う。

(4) セキュリティに関する契約の在り方の検討について

- 資料3の22ページのセキュリティに関する契約は、関心が高いが、難しいところ。製造物の欠陥に対してはPL法が

適用されるが、ソフトウェアは対象とはならない。ソフトウェアにおけるセキュリティの責任は誰にあるのか。判例が増えてくれば判断基準も定まってくるが、現状は判例も多くない。保険は賠償責任が確定しないと保険金が支払えないので早期解決を図ることができない。実務ではベンダと顧客の力関係で微妙なお金を支払わざるを得ないといったこともおきている。これが、サイバーリスク保険が普及しない一因にもなっていると考える。

- ベンダはシステムを作ってユーザに納めているので、システムに後から何らかのセキュリティ上の問題が見つかった場合、ユーザはベンダが対応すべきと言う。一方で、ベンダは使っているユーザ側が対策を講じるべきだと言う。他人任せになっているため、どちらもサイバーリスク保険に加入しない、ということになる。結果として、保険によるリスクの移転ができていないこととなっている。このあたりの整理をはっきりさせることで、責任の所在も見えてきて、ベンダやユーザのセキュリティに対する意識も変わってくるように思う。

(5) 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、非常に期待している。2年目は、生活系サプライチェーン、電力や鉄道等、街の機能を支えているメンテナンスや配管とかに携わっている人達をターゲットにしていったら良いのではないか。スマートシティの関係では、サイバー攻撃を受けて都市機能が麻痺するリスクがある。こういう観点では、地場の中小企業が深く関わる。地方の中小企業の方のリテラシー向上を進めていかないと、スマートシティは上手くいかない。そこに対するリーチ、スマホ安全教室のような形で広げていくことはできないか。
- サイバーセキュリティお助け隊の状況として、やはり、侵入ありきとか、事後対応の様な話を伝えるのが、非常に難しい。アンチウィルス入れている、人がいない等の意見が多い。
- お助け隊は、いろいろな地域で特性に応じて取り組むことも大変重要だと思うが、地域に拘らない業種という切り口で取り組むこともあるのではないか。例えばヘルスケアデータは、病院やクリニックという日本全国に同な業態の中小企業が何千社とあると捉えることができる。その情報セキュリティをどう守るのかという観点で考えることや、こういう分野・業界に横断的な仕組みを取り入れるということを考えても良いのではないか。今後の実証等で、こうした観点を取り入れて頂くことも良いのではないかと思う。

(6) 中小企業向け製品・サービスの検証について

- オールジャパンで、例えば社会インフラを中小企業まで、サプライチェーンの信頼性を製造プロセスも含めて確保した状態で作れる状況は、かなり強みになると思う。どこの国でも、それは課題になってきていて、規格やガイドラインに記載されているが、現実的にできている国はまだほとんど無い。中小企業に着目して強化していこうという方向性は、非常に良いと思っている。
- 中小企業に対応することが大変重要だと思っている。そこの穴を塞ぐことは、プリミティブなことかもしれないが、中小企業が対策を講ずることは日本の産業に効果があると思う。中小企業における穴を塞ぐ観点は非常に重要。
- 中小企業にも、大きく二つぐらいの取組がある。所謂、大企業からの下請け的にやる仕事や製品であれば、要求された仕様に対応していれば良い。一方で自主的にやっている事業に対しては、例えばメガリコール等を回避するために、セキュリティや品質も含めた対策、トレーサビリティをしっかり確保することは、自分自身を守るためのメリットになるはず。
- 日本へのサイバー攻撃は増えている。中小企業を含めて、ムーブを起こさないといけない。それには今がチャンス。今この時期でこれから多くなっていく、注目もある、関心も上がる、というときに大きなものを立ち上げるのは良いこと。勇気を持ってもう一歩出るようなことを、ムーブとして起こしていかないといけない時期なのではないか。

(7) コラボレーション・プラットフォームについて

- 地方版コラボレーション・プラットフォームについてだが、例えば、中部地方だけでコラボレーション・プラットフォームをやっても、セキュリティのサービス提供者が、ほとんどいない。中部地方は、モノ作り企業の集まりなので、そういう

企業だけで集まっても、あまりコラボレーションが生まれない。東京の新しいものを是非、愛知、中部の方へもってきて頂きたい。二次、三次のサプライヤーは、そう簡単には東京へ来られない。是非、よろしくお願いしたい。

- 中部地方は、製造業が多いので、製造関係のIoTに関するようなところを教えて頂けると、大変助かる。私共の関係の企業は、モビリティカンパニーになるという方向でやっている。そのような新しいサービスをお持ち頂けると、皆興味があると思う。

(8) その他

- 責任と資金の取組も検討してもらいたい。責任の問題については、責任を引き受けるほど、ユーザはアウトソーシングするので、ベンダは多くの責任を負いたいが、それに見合う資金が来ないため、サービスレベルを落とさざるを得ないということがある。今の原理からすれば、責任分界点をはっきりさせなければならないが、分界点をはっきりさせればコストがかかる。責任分界点をはっきりさせる方向だけではなく、責任分界点をいい加減にして、どこかが引き受ける、そういう社会的なインフラを作っていく方向もある。その資金をファンディングするような仕組みを皆で検討したらどうだろうか。サイバーセキュリティは、リスク前提なので、そういうファンディングのところにある程度責任を負わせる等、責任転嫁の仕組みも考える必要があるだろう。
- サイバーセキュリティは、社会インフラとしてのサービスになっていく。サービスの提供者には、きちっとした責任感を持ってもらう必要がある。様々な資格制度やグレードの表示をする訳だが、駄目なものは駄目と社会が分かるような、厳しい責任感を持ったビジネス業界に育てていく必要がある。
- 我々の取組は二つの方向を見る必要がある。一つは、責任の問題で、責任のある人が、賠償しなければいけないとか、その費用を払うだとか、そういう理屈は徹底させる必要がある。それは、保険領域で、常にいわれていることだと思う。一方で、サイバーセキュリティは、日本や世界を支え、それを支える日本の事業者やビジネスを育てるという社会基盤をつくる、というところがあって、そこでは、あまり厳密に責任を区分するという商品の作り方は、馴染まないと思う。保険の方でも、ソーシャル・ファンディングや、社会保険のような形で社会リスクに対する保険制度を作っていく等の取組を加速して頂いて、そういうところへの役所の関わりも強化して頂けると良いのではないか。
- サイバーセキュリティについては、日本全体を豊かにする、日本の事業者の国際競争力を高めるという、産業政策の下での話だということを意識した上で、サイバーセキュリティに関する非競争領域を強化するという明確な認識の下に、この問題を進める必要がある。
- 非競争領域と、競争できる領域を緻密に分けて考えていく必要がある。ターゲットをある程度絞って議論するということが必要ではないか。経営者に、それぞれの個社のサイバーセキュリティ領域の現実、欠けている状況を見せていく、こういう取組は、非競争領域でやるべきこと。
- 民間で推進できるようなお金の流れも作っていく必要がある。著作権の仕組みと同じように、ベンダも製品一つ売る毎に、ある程度の拠出をして、共通の非競争領域の取組をするためのファンドを作るとかを、やっても良いのではないか。また、民間が非競争領域を協力して進めていく仕組みを作る。例えばISACもその例だし、いま役所がプラットフォームをつくっているが、民間で推進できるようなお金の流れも作っていく必要があるのではないか。
- 非競争領域をつくって、そこで民間が元気良く活動することが、本当の意味での競争力を強化することになると思うので、検討してはどうか。
- 中小企業を含めた全体の社会インフラ強化ということが、国力としてできれば、競争力になるのではないか。そのために、非競争領域としてのファンドの使い方を、しっかり議論できていくと、例えば、それがトラスト基盤になるのかもしれないが、信頼できるメーカー群、取引先群をしっかり管理する仕組みができ上がってきて、オールジャパンとしてのメリットになるのではないかと思う。非競争領域でのファンドの話は、是非、社会インフラを強化する観点で検討されると、後押しになるのではないかと思う。
- 日本的な感じていくと、皆でやろうというのが一番やりやすそうだという感じがする。一年に一回、二回、そういうファンドで、皆で集って、お金も出し合って、その中でペネトレーションテスト等を行って公表もしていく、というイメージかと

思う。それを何処がやるか、というと、きっかけとして国が一番良いかと思った。先程のファンドは、広がりも見えてくるので、皆参加していって、それこそオールジャパンで、やっていく第一段階になりそうだと思った。最初数社、意識のあるところが集まって、お金も出していくということかと思うが、凄く良いと思う。

- スピードの観点からいうと、一番重要な経営層に、サイバーセキュリティの重要性を訴えないと、いろいろな施策があっても動けない。現場の話を経営層の人が、しっかりと分かることが重要で、公表することも今後重要になってくる。簡単なものでも良いので、アピールするところを作っても良いのではないか。まだ意識が高い経営者は少ないと思う。それを広げていかなければいけない、そこのアプローチが足りないのではと感じた。
- サイバーセキュリティの重要性を経営者に啓蒙していくことについては、サイバーセキュリティ経営ガイドラインはもちろん、サイバーお助け隊事業、ここの啓蒙施策など、多面的に繰り返し行っていくことが肝要と感じている。

自由討議の最後に、國領座長から以下のとおり総括がなされた。

- 本日は、非競争というキーワードが出てきて、それをファンディングの仕掛け作りも考えて大きく動かす、地方も含めて、経営者も含めて、皆で参加していかないと、この話は駄目なところだが、その求心力をどうやって作っていくか、ということだったと思う。結論にいきなり飛びつくと危ないが、そういうような知恵を働かせる必要がある。
- 公表のインセンティブをどうやって作っていくか、また、皆で参加していかないと動かない話を、どうやって動かすのか等、非常に多くの論点を出して頂けた。活発なご議論ありがとうございました。

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