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2回) 議事要旨

1. 日時・場所

日時:平成30年8月9日(木) 13時00分～15時00分

場所:経済産業省 本館17階東8 第1共用会議室

2. 出席者

委員 :國領委員(座長)、東委員、飯島委員、石井委員(代理:田中様)、石原委員(代理:教学様)、稲垣委員、鵜飼委員(代理:金居様)、鴨田委員、栗原委員、篠田委員(欠席)、手塚委員、花見委員(代理:山田様)、古田委員、宮澤委員、三輪委員、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、商務情報政策局 三角大臣官房審議官、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

冒頭、西山局長から以下のとおり挨拶。

・ 産業サイバーセキュリティ研究会で活発な議論を行って頂いており、中でもWG3は特に活発な議論がなされていると承っている。

・ サイバーセキュリティを進めていく上で、広い意味で日本に根付いたサービスや製品がきちんと外へ出ていかないと、単なるルール作りに終わってしまう。その点は、当省にとっても大きな役割であると思うので、ぜひ、皆様の活発な議論を通じて、また、私どもも色々な努力をさせて頂き、具体的なビジネスの創生につなげていきたいと思っている。

事務局から資料3について説明の後、自由討議を行った。委員からの意見は以下のとおり。

(1) 全体について

・ 報告された取組はスピード感があり、コラボレーション・プラットフォームの設置、検証基盤の検討などこれまでの議論内容が踏まえられている。

・ サイバーセキュリティの問題に対して、日本は海外よりも遅れている印象があるため、立ち上がって進んでいくのは素晴らしい。2020年はハッカーの舞台でもあるというのを感じており、できるだけ早い段階でやれることをやっていくことが重要であると思っている。

(2) 責任分界の課題について

・ ユーザ企業は、サイバー攻撃にあった事象は、システムベンダにお願いしていて、保証してもらうから、サイバー保険に加入しないという企業が多い。ベンダからしてみると、ユーザ企業がサイバー攻撃にあったとしても、保証すると

は、契約上書いていない。サイバー保険の加入者の業種は、システム系が40%位で、情報サービス業者など開発側の企業の加入率が伸びてきている。それは、ベンダがしっかりしたセキュアな商材を作っておかないとユーザから責任を問われるという気持ちの現れである。責任分界の解決策として、保険がお役に立てれば良いと思っている。

- 現在の法体系では、一対一で取引し、何か問題が生じた時に、お互いの責任について因果関係を一つ一つ確定し、相手に責任があるときは賠償を促して始めて財貨が還流するといった構造になっている。このような構造の課題は、サプライチェーンの中で、誰にどれくらいの責任があるのかが分からない。産業育成なので、責任を取らないという仕組みが必要で、財貨を流す、それからたまりが必要、しかもそれが継続する必要がある。まずは産業構造の中にアプライして、最終的には、責任が明確化した段階ではその人に責任が追及できるという風な仕組み、今までの近代的なやり方を併用させていかないといけない。今、ものすごいスピードで、ものすごい数の人たちが結びついて、責任の分界点を作ろうとしても、おそらく不明確になる。そのようなことを、世界中がやっている中で、日本の売りは何なのかというと、例えば、そういった新しい仕組みを作って、サイバーセキュリティをオールジャパンでやろうとしているのだったら、サイバーセキュリティ産業を支える財務基盤、あるいは財政基盤をオールジャパンで作ること。そのような発想のものを作っていくと、安心して産業界も参加でき、保険の方も受けられる。保険の方も、厳格にはやらないようする、再保険を活用するなど、リスクを少し考えてもらえると良い。金の流れもオールジャパンで考えるということを一緒に、やっていくと良いのではないか。この会は、日本のサイバーセキュリティ産業の経営会議みたいな話であるため、金融界をぜひ巻き込んで、考えてもらえると良いと思う。
- 責任分界が課題となっている要因として、オペレーティングリースが不透明だという点があるが、中小企業ではリースでしか、オペレーションができないという世界もあり、あえて不透明にしなければならない領域もあるかと思う。リース業界が考え、中小の工場へ導入するサービスも徐々に検討されているので、その辺りで入れる人達に負担がないようファイナンスサービスをする方々に、実際どういうニーズがあるのか、新商品を作るとしたらどうするべきか等を訊いていくと、見えてくるものがあると思う。
- 学に対しては、人材育成や資格の話をもっとしていただけると良い。民のところで考えなければいけないのは、ベンダとユーザ企業の間で契約する話もあるが、そこで保険などを絡ませることで、民の中でもエコシステムの様な広がりが出てくると良い形になるのではないかと感じている。
- 責任範囲の明確化という話があったが、サイバーセキュリティ経営ガイドラインには、サプライチェーンの委託元が委託先に対してしっかりセキュリティ対策を求め、監督しなければならないと強く書いてある。例えば、あるサプライチェーンの最上流の会社から、CSIRT と SOC を整備するよう今大号令が出ているが、内容が具体的なものでないため、各社各様で取り組んでいる状況。具体的に何をするのか提示してあげることが大事だと思う。

(3)検証基盤について

- 評価を利用する事業者がある程度増えていく段階で、評価に対する社会的な期待とのギャップについて、リスクも含めて正確に公表していく必要がある。社会の期待をある程度鮮明にしないと、評価を受審する事業者、または受審した結論を用いる事業者の期待とギャップが生じ、制度自体が陳腐化してしまう可能性がある。
- 製品の有効性検証は、実ユーザの観点で見ると、実績や性能も重要だが、やはり保守が重要。我々ユーザはいかに困ったときに助けてくれるかが重要で、保守体制をどれだけ持っているかが、実際に製品を選ぶ際に重要なポイントとなっているため、その点もご考慮いただけるとありがたい。
- セキュリティの商材は、プリベンションとディテクションなど、状況に応じて様々な商品構成があり、単純な検証環境や、テストのパターンで各々の商品の有効性をクリアにするのは、難しい。検証でどこまでカバーするのかの考え方は、2つあると思っている。何らかのセキュリティ体系をベースに、何か指針に頼るというのが一つの方法。もうひとつは、産業育成という観点をベースに、どの産業を優先するのか優先順位をつけ、やれる範囲の製品やサービスを絞って、そこに集中して実施していく必要があると思っている。

- 検証対象となる製品について、特にサービスという視点も含める必要がある。今、製品とサービスがかなり融合してきており、それらがクラウド上でどのように実現されるかという視点である。実際に政府情報システムでもクラウド・バイ・デフォルト という話が出て来ており、今後一層クラウド化が進む。情報システムを実現する環境が変ってきている、という一つの潮目だと考えられる。そういった中で、従来のセキュリティ・プロダクト・ソフトウエア（製品）とサービスの融合という話がある。ベンチャー等が本当に競争力のある製品を提供していこうとすると、如何に新しい機能を作り実現していくのか、言い換えると、製品とサービスを如何に融合させるのか、さらにはクラウド上の生態系（エコシステム）でそれらをどのように上手く活用していくのかという考えの下で、差別化を実現していくべきである。
- 有効性検証対象製品について、4区分の対象製品群が示され、それらからの「選定」という資料表記となっている。例えば経済産業省がこの部分は少してこ入れするよ、というように捉えられると、ミスリードとは言わないが、ベンチャー企業もその方向性に流れてしまうのではないか？　ここは「戦略性」という言葉がある意味で「選ぶ」、つまり「捨てる」ということを考えれば、日本として一番得意なところをどうするべきか、ということとも関係してくる。16ページに記載された製品群はあくまで例示であるべきだと思う。セキュリティ製品やサービスは、新しい機能・概念がどんどん出現してくる。EDRというのは一つの例で、数年前にはなかった概念だが、現在はクラウド環境下で利用されていて、今ピークになろうとしているので、これから追ってもいけない話。製品の選定にあたっては、差別化を持った製品、サービスをどのように新しく創出していくのかという観点が大事だと思っている。
- 有効性検証においては、悪意のある攻撃を見つけ出すという検知力が大切な評価の視点であるが、同時に、攻撃ではないものを誤って攻撃と検知してしまうフォールスポジティブの割合が小さいことも重要な評価の視点となる。誤検知が運用負荷を高める観点から極めてマイナスだということを考えると、フォールスポジティブを低くするという性能強化も求められる。これらの視点に対する有効性検証には、どちらも攻撃に対するインテリジェンスをどれだけ広範囲に活用した検証を行ったかが求められる。特にベンチャー等の利用者が検証環境を活用する際に、いかに広範な攻撃関連インテリジェンスを基に客観的に評価を行ったかを示せないと評価結果に対する信頼性というものが非常に低いものになる。
- 加えて、特に最近の攻撃は、攻撃元のURLが短時間で変更されるなど攻撃関連情報の陳腐化が早い。検証環境で整備すべき評価用の攻撃インテリジェンスに対して、時間軸での新鮮さへの配慮が求められる。このような評価データや検証方法に対して、共通な下支えとしての基盤は非常に有効であり、共通で整備すべきである。
- ホワイトハッカーの実攻撃検証の検討は、積極的に行っていただきたい。ホワイトハッカーというと、個人を想定するが、ホワイトハッカーの能力を提供している事業者もいるように、ユーザだけでなくて、ベンダもいるし、ベンダを支える人材もあるし、民もあれば官もあるし、大学もあると思う。ホワイトハッカーによる攻撃検証の基盤を、攻撃の事実だけでなくて、それを支える経済的な動きや教育の提供など、少し関係者を整理した上で、日本全体の能力を高めていく仕組みを検討いただけると、成果が上がってくると思う。
- ホワイトハッカーを使っていくときに、まず必要なのは、人数であるが、これを早急に集めるのは難しい。かなりスピード感をもってホワイトハッカーの育成を進めないといけない。一方で、ハッキングする人の倫理性は、難しい問題であり、ホワイトハッカーの選定を相当センシティブにしっかり行う必要がある。
- ホワイトハッカーについて、実際困っているのは人材不足、リソースが足りないということ。ハッカーの性格として、問題を見つけると外に向けて早く言いたい、という特性がある。企業側としっかりと連携をして、対策が打てるようになってから公表するなど、信頼できるようなハッカーを国が認定して作っていただけると大変ありがたい。
- ホワイトハッカーの大量育成には非常にリスクが伴う。日本は日本人を信用しすぎで、非常に危険な組織に属している人が、その中でリクルーティング、仲間を増やすなどの活動をしている。アメリカでは、セキュリティクリアランスという制度があって、その中でシークレットやトップシークレット、コンフィデンスといった情報にアクセスできる権限が与えられる。先進国の中ではおそらく日本が一番遅れているので、安易に考えることなく、ぜひ真剣に取り組んで欲しい。
- ホワイトハッカーの実攻撃検証は、信頼できるホワイトハッカーを探し出し、承認し、検証を進める仕組みをどのように

整えるかという点が難しい。使いたい人は当然いるが、使うことによって、何らかのお墨付きを与えるなど、経済合理性も持たないといけない。

- ホワイトハッカーの技術交流については、お客様の関心が高く、ニーズとしてはあると思う一方で、ハッカーそのものの人数が少ないので正直、依頼が重なるとお断りせざるを得ないというのが課題になっている。この仕組みをどう発展させていくのかは、検討が必要であると思っている。
- ハッカーにお願いして穴を見つけたときに、そのハッカーはその穴を直せるかは、別の問題で、直す方法を考えるのが別の技術者だったりする。また、日本で成果物の品質を上げるために特に重要なのは、開発プロセス。たまたま試験をしたシステムで穴を見つけたときに、この穴を二度と作らないために社内の開発プロセスをどう直すか、社内のセキュリティ基準をどう変えるかというところまでしっかり直して、再発防止をするというのは、日本企業では凄く考えられているため、ハッカーとは違うタイプの人間が必要になることがある。国として、「ホワイトハッカーの実攻撃検証」に何らかの費用を支援していただけるとしたときに、穴を見つけるまでの支援に留まらず、会社の中でどう対策して、どう再発防止をするかまで、手厚く支援するというのが重要なのではないか。
- 侵入テストも増えてきている中で、技術者がたくさんいるかというと、日本国内に限らず、ワールドワイドでも過剰にいるわけではないので、どのようなゴールを設定するのかという議論した方が良い。
- 組込みソフトウェアやIoT分野のホワイトハッカー人材が必要である。個人的に気になっているのは、AI環境。旧来の手続き型プログラミング言語やセキュリティ運用上の穴を見つけるハッカー人材はもちろん必要だが、より広い意味でブロックチェーンやチップの脆弱性、ディープラーニングを用いたAIシステムの脆弱性を見つけることができるホワイトハッカーも必要になる。これらのホワイトハッカーに求められるスキル・技量は、従来と全く異なる内容・レベルなので、その分野に精通した人材も必要。
- ホワイトハッカーがバグを出したときや、脆弱性を見つけたときに、結果を公表して良いのか、いけないのか、そういった観点からも政府として検討してほしい。
- 日本の特徴であるが、メイドインジャパンにすごく自信がある。セキュリティに対して取り組んでいる企業が、自分たちのバグを公表しても、しっかりと製品と向かいあっている企業を評価していくという後ろ盾がないと、どれだけハッキングや脆弱性を見つけても、なかなか先に進まないと思う。
- ホワイトハッカーの実攻撃検証は、各事業者にとって大変ニーズがあると思っている。資料13ページに、例えば重要産業のセキュリティを検証するとあるが、ここでいう日本の重要産業は何なのか、守った方が良い重要情報インフラやネットワークの定義などの議論から始めて、守るべきものは何かが認識がされていくのが良いと思う。ぜひ、どういう産業、どういうシステム、あるいはどういう情報を守っていくかという共通認識と、そこに対して個々の企業なのか、国として検証環境を作るのか、あるいは、ハッカーとのマッチングを作っていくのかという仕組みをぜひ検討していただきたい。
- いわゆる評価基準という形になると、パブリックに共有していくことになるが、これは攻撃者から見ると、このレベルのものは通っていく、逆にこの評価の裏の穴を、ある意味でメッセージとして出すことになるので、評価基準の共有方法を考えていく必要があると思う。
- 製品やサービスの有効性検証の対象を国内の製品に限定せずに、海外の製品が日本で流通する際や海外から攻撃をされる際などを想定し、グローバルな問題として考えるべきではないか。
- 機能要件の考え方、さらに有効性検証の有効性とは一体何であるかというところを、エクスプリシット仕様化していかないと評価基準が見えてこない。特に第三者認証的な評価が大事になるので、日本の中でのコンセンサス、国際的なコンセンサスも最終的にとる必要があると思う。
- 標準のセキュリティという観点からCC認証などと、どのように住み分けていくか等、他の全体的な標準化、評価形態、評価系との連携について詰めていっていただきたい。
- セキュリティ製品の中には、技術論が確立されていない製品もあるため、基準を一律に作って多くの機器を、その基

準で評価すると、検証する人によって成果がぶれることがあると思う。一方で、確立されている領域では、検証基準を方法論としてドキュメント化し、共有することで、検証側を育成していくことができると思う。

- ベンダ側が最も欲しいのは、お客様や官公庁で実際に導入されて成果をあげた等の実際にユーザが使ったという事績。
- 事業者の立場から、一番気になるのは、検証基盤を導入する人のモチベーション。つまり、製品を提供する人であれば、どうして製品をセキュアにするのか、あるいは、製品サービスの提供を受ける側では、どうしてそのサービスの提供を受けるのか、というところに合理的な理由や動機付けが欲しい。
- 海外ベンダの事例で、一回攻撃されて業務を再開するときにレッドチーム・オペレーションを必須にする、あるいはレッドチーム・オペレーションを受けていると、サイバー保険料を安くする等、面白そうな例がいくつかある。長い目で見ると民と民で進めていく話であり、官の方に対しては規制みたいなものや法律論の見直しをお願いしたいと思っている。

(3) コラボレーション・プラットフォームについて

- セキュリティ関係者と、実際にもの作りをしている人との会話が非常に重要だと感じている。今回始めていただいたコラボレーション・プラットフォームの中で、もの作りをしている人とセキュリティをしている人との対話が出来ると、産業の発展に資するのではないか。
- コラボレーション・プラットフォームに参加して、供給側もユーザ側も他社の状況を知らないため、ネットワークを構築して情報を共有したいというニーズが参加者に強くあったと思う。また、今後の実施方法を考えた時に、参加者の目的意識に則して、例えば地方や業界などの切り口で、他社の取組状況などを共有、情報交換していくというのは、有効なのではないか。
- コラボレーション・プラットフォームで、今までお会いできなかった製品ベンダの方々にもお会いできる機会があり、大変参考になっている。
- コラボレーション・プラットフォームの場で懇親会を含めて名刺交換をしたが、そこで知り合った方と、具体的な話を進めようとしている。あれだけ短い期間に名刺交換をしただけで、これだけの出会いがあり、非常に貴重な機会だと思っている。一方で、ニーズとシーズという観点で、出会いをもっと効率的にできるやり方を検討する必要があると思う。
- 業界によって感度が違うと思うが、毎月開催というのは頻度が多いという印象を持っている。コミュニティ形成だと、どの会社も基本的に決まった人を選ぶと思うが、その立場の人が毎月出るのは調整が難しい場合もあり、トピックがなくなっていって、中身が薄くなるといったことを懸念している。

(5) その他

- 情報セキュリティシステム監査企業台帳を情報セキュリティサービス審査登録制度に移行していくのは良いと思う。一方で、システム監査は、セキュリティ問題とはまったく違った領域のシステム監査も多くあるため、慎重に考えていかないといけない。
- サイバーセキュリティ分野の施策について、事業者が参加し、社会に風土をつくり、色々なことに挑戦するが、それらに必要なお金を継続的に供給できる仕組みも合わせて考えてもらいたい。
- サイバーセキュリティ産業を立ち上げるのに必要な初期投資をどうするかということを議論していただきたい。例えば医療分野では、今は危機感があり、怖いからネットワークに繋ぎたくないと、現場の人は話していて、そのときに安全なネットワーク引くのか、WANを使うのかというオペレーションの問題になっていく。ただ一方で、遠隔医療の話が出てきて、使わざるを得ない。そうなると、オペレーションが回らないのに、どんどん効率化してきて全体的なコストの削減ということで地方自治体が、事業コスト削減で、どんどんIoT化していき、結果コスト削減できたときにセキュリティの話はどうだろうとなっても、地方税くらいしかなくて、お金がそこにまわせないという観点もひとつあると思う。産業側で

見ると、全面的に中小企業もIoT化してきている中で、保険の話もあれば、リースの話もあり、IoT設備をどんどんリーシングしていくという話もある。リースの業界に関わっていくが、オペレーティングリースで、立ち上がっていないところをリーシングでカバーするというのは、ひとつの観点としてあり、保険の共有の観点もある。この産業サイバーセキュリティを立ち上げるなかでビジョン、ロードマップのようなものがあったら良いのではないかと思う。

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