第3回 産業サイバーセキュリティ研究会 議事要旨

1. 日時・場所

日時:平成31年4月19日(金) 16時00分～16時55分

場所:経経済産業省 本館 17階 国際会議室

2. 出席者

委員 :村井委員(座長)、宮下様(石原委員代理)、阿部様(泉澤委員代理)、遠藤委員、小林委員、篠原委員、中西委員、船橋委員、渡辺委員

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 前田センター長、
内閣官房 山内内閣審議官(内閣サイバーセキュリティセンター副センター長)、
警察庁 長官官房 高木サイバーセキュリティ・情報化審議官、
金融庁 総合政策局 水口審議官(サイバーセキュリティ・総合政策局担当)、
総務省 竹内サイバーセキュリティ統括官、
外務省 総合外交政策局 大鷹審議官(サイバー政策担当大使)、
文部科学省 大臣官房 菱山サイバーセキュリティ・政策立案総括審議官、
厚生労働省 大臣官房 椿サイバーセキュリティ・情報化審議官、
農林水産省 大臣官房 山本サイバーセキュリティ・情報化審議官、
国土交通省 大臣官房 大野サイバーセキュリティ・情報化審議官、
防衛省防衛装備庁 長官官房 藤井審議官

経済産業省:世耕経済産業大臣、商務情報政策局 西山局長、三角サイバーセキュリティ・情報化審議官、
成田審議官、奥家サイバーセキュリティ課長、通商政策局 福永サイバー国際経済政策統括調整官、
製造産業局 井上局長、産業保安グループ 米田審議官、
資源エネルギー庁 電力・ガス事業部 村瀬部長、中小企業庁 経営支援部 那須野部長

3. 配付資料

資料1 議事次第・配付資料一覧

資料2 委員等名簿

資料3 最近のサイバーセキュリティに係る国際動向(事務局説明資料)

資料4 産業サイバーセキュリティの加速化指針～アクションプランの深化・拡大～(事務局説明資料)

4. 議事内容

冒頭、世耕経済産業大臣から以下の通り挨拶。

- デジタル領域の信頼を脅かすサイバー攻撃が日々高度化して、この一年の間だけでも様々に事案が発生し、その都度、色々な新しい手口、高度化した手口が出てきている。データフリーフローwithトラストを実現していくためには、こうした脅威に対抗、対応していかなければならない。経産省では、他省庁と連携をして、昨年この研究会でまとめたアクションプランを実行して、大きく前進をさせてきた。本日は、このアクションプランを深化拡大して取り組みを加速化していくための3つの指針を提示する。
- 一つ目はグローバルをリードしていくために国際的に認知が進むサイバー・フィジカル・セキュリティ対策フレームワー

クを軸に、産業分野別の実装を進めてデータ革新に向けたグローバルな動きを先取りする。二つ目は信頼の価値を創出して、これをビジネスにつなげて行く、いわばChecked by Japanという旗を掲げて、セキュリティビジネスの成長を促進して行く。三つ目は、セキュリティの取り組みを中小企業や地域まで展開するため、中小企業向けの相談、駆けつけ支援体制を構築するサイバーセキュリティお助け隊や、地域の産業を支えている高等専門学校との連携強化をすすめていきたいと思う。

- 日本の産学を最前線で引っ張って頂いている委員の皆様から、この3つの方向性にとらわれることなく、また、経産省の分野に限らず、政府全体の取り組みに対して大所高所から忌憚のないご意見を頂きたい。

次に、村井座長から以下のとおり挨拶。

- コネクティッドインダストリーでは、全産業が連結していくことから産業面でのアドバンテージは出てくるが、そのためにサプライチェーンを含めて、色々なリスクも出てくるだろう。また、グローバルに日本の重要性がどこにあるかというと、まさに日本の産業が信頼、あるいは品質といったものに対して拘りを持って成長してきた背景があると思う。それが、どのようにしてグローバルなサイバースペースの中で日本の貢献となり、あるいは日本の産業が世界で活躍をする際の強みになるかということが大変重要な観点になるのではないかと思う。
- この分野の技術は毎日進歩する。新しいものが出てきて、新しいものに目をつけたグローバルなサービスが毎日出てくる。そうすると、メディア、農業、教育、医薬等、あらゆる分野が毎日変わっていく。変わると大きく発展していくが、アブユーズ（濫用）する者が必ず出てくる。これがサイバーセキュリティのバランスであり、常に新しいものを議論できる柔軟な体制も必要だと思う。そういうことも含めて今日は活発な議論をよろしくお願いする。

事務局から、資料3、資料4についての説明に続き、以下のとおり自由討議を行った。

各委員からの意見は以下のとおり。

<u>サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）について</u>

- CPSFを具体的に動かしていくために、タスクフォースが設立されるということだが、お願いは、機能を作り上げるためだけのタスクフォースではなく、常にこのタスクフォースが、機能を進化させるためのアクセレーションの良いタスクフォースにして頂きたい。
- CPSFのどこを標準化するか、狙いどころを明確にすることも重要ではないか。

<u>Checked by Japanについて</u>

- 今回は装置のChecked by Japanだと思うが、装置だけでは不十分だと思っている。装置にかかわるオペレーションとかサイバーセキュリティのレリジエンスの仕組とかを含めたトータルのChecked by Japanということをお考え頂きたい。また、自ら使い安全であることを発信することもお願いしたい。
- 資料4にChecked byというところにProved byと小さく書いてあるが、Proven inあるいはverified in Japanというのも日本で証明されているから安心でしょう、くらいの意味で良いと思う。
- Checked by Japan の考え方はすばらしいと思うが、Checked by Japan だと政府が全部やっております、というようなことで反作用がひとつあると思う。

人材について

- 製品のセキュリティというものを守るためには、ペネトレーションやリバースエンジニアリングが必要だが、この辺ができる人材が非常に少ない。高度なサイバーセキュリティに関する人材育成は、ぜひお願い申し上げたい。これは官民一体とならないといけないところなので、我々も協力申し上げる。また学も含めて仕組みを作り上げていくために、協力していきたいと思う。
- 産業分野毎に、その分野の専門知識を持ったセキュリティ要員を育てる取り組みが必要。特に製造業では、インフォメーション・テクノロジーとオペレーショナル・テクノロジーの両方を兼ね備えた人材が鍵になる、という状況の中で人材育成を考えるべきである。
- 昨年度に実施されたサイバーセキュリティ経営強化パッケージ、それからサイバーセキュリティ人材育成パッケージは、ぜひとも継続して実施をして頂きたいと思う。

中小企業のセキュリティ対策について

- 攻撃者側から見ると一番弱いところから攻めるというのが常套手段なので、やはり日本の90%以上を占めている中小企業さん、ここが攻めやすいというのは確かだと思う。今回のお助け隊というのを作って頂いたが、お助け隊の最後のところの現場の人材が今後、不足してくると思う。シニア人材の登用や、女性などを含めて地域でお助け隊を動かして頂ける人材を、どうやって集めていったら良いのか、その辺も含めてご議論させて頂ければありがたい。
- 中小企業へのセキュリティ対策の支援を大分広げたということだが、網羅性が結構大事なので、どこかでモニタリングできる仕組みをご検討頂きたい。
- 中小企業のIT環境は様々でサイバー被害の実態は極めて判りにくい状況にある。今回、お助け隊という分かりやすい窓口を設けられたということで、小さなことでも相談しやすくなり、様々な情報も得られるようになったと思っている。
- セキュリティアクションをIT導入補助金の要件とすることで、6万7千もの中小企業がIT導入と同時にセキュリティについて考えるきっかけをつくったことは、大変意義あることと思っている。また、宣言した中小企業が継続してセキュリティに取り組む次のステップに進むための工夫について、今後議論することが必要だと思う。
- サプライヤーについては、現状では発注側企業が発注先企業に対しセキュリティ確保を依頼しており、各企業が個別にセキュリティを守る様な形で実施している実態がある。中小企業に対して、最低限必要なセキュリティの共通指針や認定制度等、これをやっておけば意味があるようなものが出来れば、個別対応が不要となり、発注側企業にとっても大きなメリットがあると考えている。
- 中小企業の社員一人ひとりが何かあったときにどういう行動に出るかということが一番大切なので、専門家によるお助け隊だけでなく、社員一人一人のサイバーセキュリティに対するリテラシーが大事であることや、どうあるべきかというメッセージを出すことが重要。

経営層の認識について

- 産業界はこの一年間振り返ってみると日本では表立った被害はないということで、経営者の意識が緩みつつあるのではないかという危機感を持っている。
- JUASでは、企業IT動向調査を実施しているが、経営者の意識が昨年度に対して若干低下している。特に大企業で、経営者の意識の低下が顕著にでてきていることに懸念をしている。一方で企業におけるサイバーセキュリティのインシデント発生状況は、2年連続低下してきている。ただ、サイバー攻撃が減っているということでは決してなく、恐らく企業におけるサイバーセキュリティ対策がきちっと出来ており、結果としてインシデント発生が抑えられているのではないかと推定している。

情報共有について

- 地方では、ITやセキュリティに関する情報が限られている。そこで、コラボレーション・プラットフォームのような取り組みを特に地方で積極的に開催して頂きたい。
- 企業間のコラボレーション、ベストプラクティスや被害に対する対応の共有等、業界を主導する協力関係、いわゆるISACのようなものが大事だと思っている。被害を受けた後の対応等で業界共通な部分があるので、中小も含めた企業間の連携をもっと加速するような施策が必要。

安全保障について

- 国の防衛サイバーセキュリティの観点から防衛大綱も、相当新しい異次元の防衛構想を出してきたときに、産業のサイバーセキュリティをこれから考えていくと、国としての何を守るのかという全体と整合性ある形で相互に共振する形で進めていく必要があるということを考えている。
- 安全保障の観点からすると日本のセキュリティ・ソフトウェアが日本を守るという形になるのが、理想だが、今はほとんどアメリカのソフトウェア。これが日本製になるように、日本の人材、かなり高度の人材育成をしていかないと、そういうふうになっていかない。そこの仕組みは重要。

最後に世耕経済産業大臣から以下の通り挨拶。

- データドリブンの社会、経済になっていくといわれている中で、また、IoT、AI、5G と色々な動きが出てくる中で、守るべきもの、守るべきポイントが無限大に広がってきており、まだ網羅的、システム的に守れていないということで、課題は多いと思っている。
- これから日本では、ビッグ・イベントがあり、さらに世界的に非常ハイ・プロファイルで狙いたくなる国にもなるわけで、そのなかで経営者、トップの意識が下がっているというのは大変心配でもある。これは、経済団体、中小企業を含めて経産省とよく連携をしてもう一度で螺子を巻きなおしていく必要があるのではないかと思う。
- 本日は、我々の方から、大きく3つの視点での議論ということを申し上げたが、議論は常にアップデートしていかないと追いつかないと思っている。我々の方でも精力的に取り組んでいくので、今後ともご指導のほどよろしくお願いする。

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